An Inquiry-Based

Introduction to Proofs

Jim Hefferon

version 1.0

Notation

$\mathbb{N}$	natural numbers $\{0,1,2,\ldots\}$
$\mathbb{Z}$, $\mathbb{Z}^+$	integers $\{\ldots,-2,-1,0,1,2,\ldots\}$, positive integers $\{1,2,\ldots\}$
$\mathbb{R}$	real numbers
$\mathbb{Q}$	rational numbers
$a \mid b$	a divides b
$a \bmod b$	the remainder when a is divided by b
$a \equiv c \pmod{b}$	a and c have the same remainder when divided by b
$\gcd(a,b)$, $\operatorname{lcm}(a,b)$	greatest common divisor, least common multiple
$a \in A$	a is an element of the set A
$\varnothing$	empty set $\{\}$
$A \subseteq B$	A is a subset of B
χ_A	characteristic function of the set A
A^{c}	complement of the set A
$A \cup B$, $A \cap B$	union, intersection of the sets
$A - B$, $A \triangle B$	difference, symmetric difference of the sets
$\lvert A \rvert$	order of the set A; the number of elements
$\mathscr{P}(A)$	power set of A; the set of all of A's subsets
$\langle x_0, x_1, \ldots \rangle$, (x_0, x_1)	sequence, ordered pair
$\operatorname{lh}(\langle x_0, x_1, \ldots \rangle)$	length of the sequence
$A_0 \times A_1 \times \cdots \times A_{n-1}$, A^n	Cartesian product of sets, product of a set with itself
$f \colon D \to C$	function with domain D and codomain C
$\operatorname{id} \colon D \to D$	identity map; $\operatorname{id}(d) = d$
$f\restriction_B$	restriction of f to a subset of the domain
$f^{-1}(c)$, $f^{-1}(A)$	inverse image of an element or subset of the codomain
$g \circ f$	function composition
f^{-1}	function inverse to f
$x \equiv y \pmod{R}$	$(x,y) \in R$ where R is an equivalence relation
$[\![x]\!]$	equivalence class containing x
$\mathcal{P}$	partition of a set
$A \sim B$	two sets with the same cardinality

Greek letters with pronounciation

character	name	character	name
α	alpha *AL-fuh*	ν	nu *NEW*
β	beta *BAY-tuh*	ξ, Ξ	xi *KSIGH*
γ, Γ	gamma *GAM-muh*	o	omicron *OM-uh-CRON*
δ, Δ	delta *DEL-tuh*	π, Π	pi *PIE*
ϵ	epsilon *EP-suh-lon*	ρ	rho *ROW*
ζ	zeta *ZAY-tuh*	σ, Σ	sigma *SIG-muh*
η	eta *AY-tuh*	τ	tau *TOW (as in cow)*
θ, Θ	theta *THAY-tuh*	υ, Υ	upsilon *OOP-suh-LON*
ι	iota *eye-OH-tuh*	ϕ, Φ	phi *FEE, or FI (as in hi)*
κ	kappa *KAP-uh*	χ	chi *KI (as in hi)*
λ, Λ	lambda *LAM-duh*	ψ, Ψ	psi *SIGH, or PSIGH*
μ	mu *MEW*	ω, Ω	omega *oh-MAY-guh*

The capitals shown are the ones that differ from Roman capitals.

PREFACE

This is a course in mathematical proof. It is for math majors, typically sophomores in the US, although since its only prerequisite is high school mathematics it can be used with first year students.

APPROACH. This course is inquiry-based (sometimes called Moore method or discovery method). This text is a sequence of exercises, along with definitions and a few remarks. Students work through the material together by proving statements or by providing examples or counterexamples. This makes each person grapple directly with the mathematics — the instructor only lightly guides, while the students pledge not to use outside sources — talking out misunderstandings, sometimes stumbling in the dark, and sometimes having beautiful flashes of insight. For these students, with this material, this is the best way to develop mathematical maturity. Besides, it is a lot of fun.

TOPICS. We cover sets, functions and relations, and elementary number theory.

We start with number theory instead of sets for the same reason that the baseball team's annual practice starts with tossing the ball and not with reading the rulebook. Math majors take readily to proving things about divisibility and primes, whereas weeks of preliminary material is less of a lure.

But the background is good stuff also and students are on board once they see where it is going. In the second and third chapters we do the other material, keeping the intellectual habits that we established at the start.

EXERCISES. As much as the material allows, nearby exercises have about the same difficulty. This standard gradually rises.

Some exercises have multiple items; these come in two types. If the items are labeled A, B, etc., then each one is hard enough to be a separate assignment. If the labels are (i), (ii), etc., then they together make a single assignment. I have students put proposed solutions on the board for the group to discuss and if the items are labelled alphabetically then I ask a different student to do each one, while for the others I ask a single student to do them all.

HOME PAGE. This book is Free; see `http://joshua.smcvt.edu/proofs`. That site has other material related to this text, including its LaTeX source.

The most important thing [is that] proving things in math [i]s a skill like any other that you get good at through practice. —Cathy O'Neil

At the first meeting of the class Moore would define the basic terms and either challenge the class to discover the relations among them, or, depending on the subject, the level, and the students, explicitly state a theorem, or two, or three. Class dismissed. Next meeting: "Mr Smith, please prove Theorem 1. Oh, you can't? Very well, Mr Jones, you? No? Mr Robinson? No? Well, let's skip Theorem 1 and come back to it later. How about Theorem 2, Mr Smith?" Someone almost always could do something. If not, class dismissed. It didn't take the class long to discover that Moore really meant it, and presently the students would be proving theorems and watching the proofs of others with the eyes of eagles. —Paul Halmos

It's a kind of art that may change lives. —Peter Schjeldahl

Jim Hefferon
Saint Michael's College
Colchester, Vermont USA
2015-Spring

Chapter 1 Numbers

We begin with results about the integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. In this chapter, "number" means integer. Some statements refer to the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ or the positive integers $\mathbb{Z}^+ = \{1, 2, \ldots\}$.

Divisibility

1.1 Definition. For two integers d, n we say that d *divides* n if there is an integer k such that $d \cdot k = n$. Here, d is the *divisor*, n is the *dividend*, and k is the *quotient*. (Alternative wordings are: d *is a factor of* n, or d *goes evenly into* n, or n *is a multiple of* d.) We denote the relationship as $d \mid n$ if d is a divisor of n or as $d \nmid n$ if it is not.

1.2 Definition. A number is *even* if it is divisible by 2, otherwise it is *odd*. (Alternative wording is that the number *has even parity* or *has odd parity*.)

The notation $d \mid n$ signifies a relationship between two numbers. It is different than the fraction d/n, which is a rational number. We can sensibly ask "Does 2 divide 5?" but "Does 2/5?" is not sensible.

1.3 Exercise. (Interaction with sign) Prove or disprove.

A. If a number is even then its negative is even. If a number is odd then its negative is odd.

B. If $d \mid a$ then $-d \mid a$ and $d \mid -a$. In addition, $d \mid |a|$ (recall that the absolute value of a number $|a|$ is a if $a \geq 0$ and is $-a$ if $a < 0$).

1.4 Exercise. (Interaction of parity and addition) Prove or disprove.

A. The sum of two evens is even. The difference of two evens is even.

B. The sum of two odds is odd. The difference of two odds is odd.

C. Where $a, b \in \mathbb{Z}$, the number $a + b$ is even if and only if $a - b$ is even.

D. Generalize the first item to arbitrary divisors.

1.5 Exercise. (Interaction of parity and multiplication) Prove the first, and prove or disprove the second.

A. The product of two evens is even. Generalize to any divisor.

B. The quotient of two evens, if it is an integer, is even.

1.6 Exercise. (Divisibility Properties) Let d, m, and n be integers. Prove each.

A. (Reflexivity) Every number divides itself.

B. Every number divides 0 while the only number that 0 divides is itself.

C. (Transitivity) If $d \mid n$ and $n \mid m$ then $d \mid m$. That is, if n divides m then so do n's divisors.

D. (Cancellation) For $d, n \in \mathbb{Z}$, if for some nonzero integer a we have that $ad \mid an$ then $d \mid n$. Conversely, if $d \mid n$ then $ad \mid an$ for all $a \in \mathbb{Z}$.

E. (Comparison) For $d, n \in \mathbb{Z}^+$, if n is a multiple of d then $n \geq d$.

F. Every number is divisible by 1. The only numbers that divide 1 are 1 and -1.

G. The largest divisor of a is $|a|$, for $a \in \mathbb{Z}$ with $a \neq 0$.

H. Every nonzero integer has only finitely many divisors.

1.7 Exercise. What conclusion can you make if $a \mid b$ and $b \mid a$?

1.8 Exercise. Suppose that $a, b, c \in \mathbb{Z}$.

A. Prove that if $a \mid b$ then $a \mid bc$ for all integers c.

B. Prove that if $a \mid b$ and $a \mid c$ then a divides the sum $b + c$ and difference $b - c$.

C. (Linearity) Prove that if $a \mid b$ and $a \mid c$ then a divides any $i \cdot b + j \cdot c$, where $i, j \in \mathbb{Z}$.

INTERLUDE: INDUCTION

Results in the prior section need only proof techniques that come naturally to people with a mathematical aptitude. However some results to follow require a technique that is less natural, mathematical induction. This section is a pause for an introduction to induction.

We will start with exercises about summations. (However, note that induction is not about summation; we start with these simply because they make good exercises.) For example, in playing with numbers many people have noticed that the odd natural numbers sum to perfect squares: $1+3=4$, $1+3+5=9$, $1+3+5+7=16$, etc. We will prove the statement, "The sum $1+3+5+\cdots+(2n+1)$ equals $(n+1)^2$."

That statement has a natural number variable n that is free, meaning that setting n to be 0, or 1, etc., gives a family of cases: $S(0)$, or $S(1)$, etc. For instance, the statement $S(1)$ asserts that $1+3$ equals 2^2. Our induction proofs will all involve statements with one free natural number variable.

These proofs have two steps. For the *base step* we will show that the statement holds for some intial number $i \in \mathbb{N}$ (sometimes there is a finite list of initial numbers). The *inductive step* is more subtle; we will show that the following implication holds.

$$\begin{array}{c}\text{If the statement holds from the initial number up to and including } n=k\\ \text{then the statement holds also in the } n=k+1 \text{ case.}\end{array} \qquad (*)$$

The *Principle of Mathematical Induction* is that completing both steps proves that the statement is true for all natural numbers greater than or equal to the initial number i.

For the example statement about odd numbers and squares, the intuition behind the principle is first that the base step directly verifies the statement for the initial number 0. Next, because we have shown that the implication $(*)$ holds in all cases, applied to the $k=0$ case it gives that the statement holds also for the number 1. That is, $(*)$ with $k=0$ says that $S(0)$ implies $S(1)$, and because we have verified the assertion $S(0)$, we conclude that $S(1)$ holds. Continuing on, $(*)$ with $k=1$ says that $S(0)$ and $S(1)$ together imply $S(2)$, so we know that $S(2)$ holds. In this way, induction bootstraps to all numbers.

Here is an induction argument for the example statement, with separate paragraphs for the base step and the inductive step.

Proof. We show that $1+3+\cdots+(2n+1)=(n+1)^2$ by induction. For the $n=0$ base step note that the sum on the left has a single term, 1, which equals the value on the right, 1^2.

For the inductive step assume that the formula is true for $n=0$, $n=1$, …, $n=k$, and consider the $n=k+1$ case. The sum is $1+3+\cdots+(2k+1)+(2(k+1)+1)=1+3+\cdots+(2k+1)+(2k+3)$. By the inductive hypothesis the statement is true in the $n=k$ case so we can substitute $1+3+\cdots+(2k+1)+(2k+3)=(k+1)^2+(2k+3)=(k^2+2k+1)+(2k+3)=(k+2)^2$. This is the required expression for the $n=k+1$ case. ∎

1.9 EXERCISE. Prove by induction.

A. $0+1+2+\cdots+n=n(n+1)/2$

B. $0+1+4+9+\cdots+n^2=n(n+1)(2n+1)/6$

C. $1+2+4+8+\cdots+2^n=2^{n+1}-1$

1.10 EXERCISE. Prove each by induction. Suppose that $a,b\in\mathbb{R}$ and that $r\in\mathbb{R}$ with $r\neq 1$.

A. (GEOMETRIC SERIES) $1+r+r^2+\cdots+r^n=(r^{n+1}-1)/(r-1)$

B. (ARITHMETIC SERIES) $b+(a+b)+(2a+b)+\cdots+(na+b)=(n(n+1)/2)\cdot a+(n+1)\cdot b$

1.11 EXERCISE. Prove by induction that $n<2^n$ for all $n\in\mathbb{N}$.

1.12 EXERCISE. Prove each by induction.

A. For all $n\in\mathbb{N}$, the number n^2+n is even.

B. For all $n\geq 2$ the number n^3-n is divisible by 6. *Hint:* use 2 for the base.

C. If $n\in\mathbb{Z}^+$ then $(1+{}^1\!/_1)\cdot(1+{}^1\!/_2)\cdots(1+{}^1\!/_n)=n+1$.

1.13 EXERCISE. Prove that $n+1$-term sums of reals commute: $a_0+a_1+\cdots+a_n=a_n+\cdots+a_0$ for all $n\geq 1$, starting from the assumption that sum of two terms commutes.

1.14 Exercise. The *Fibonacci number sequence* $0,1,1,2,3,5,8,13,\ldots$ is defined by the condition that each succeeding number is the sum of the prior two $f_{n+1}=f_n+f_{n-1}$, subject to $f_0=0$ and $f_1=1$. Where does the following argument, purporting to show that all Fibonacci numbers are even, go wrong? "The base case is clear since 0 is even. For the inductive step, assume the statement is true for all cases up to and including $n=k$. By definition the next case f_{k+1} is the sum of the two prior numbers, which by the inductive hypothesis are both even. Thus their sum is even."

While many induction arguments use only the the $n=k$ part of the inductive hypothesis, some break from that pattern.

1.15 Exercise. The game of Nim starts with two piles, each containing n chips. The two players take turns picking a pile and removing some nonzero number of chips. The winner is the one who takes the final chip. Prove that the second player always wins by: whatever number of chips the first player takes from one pile, the second player takes the same number from the other pile.

1.16 Definition. The *Least Number Principle*, or *Well-ordering Principle*, is that any nonempty subset of the natural numbers has a least element.

1.17 Exercise. Show that the Principle of Induction implies the Least Number Principle. *Hint:* show by induction that if a set of natural numbers does not have a least element then it is empty.

Division

1.18 Exercise. (Division Theorem) For any integers a,b with $b>0$ there are unique integers q,r such that $a=bq+r$ and $0\leq r<b$. Here, a is called the *dividend* and b is the *divisor*, while q is the *quotient* and r is the *remainder*. We prove this in three stages.

A. Show that q and r are unique, assuming that they exist. *Hint:* one way to proceed is to suppose that $a=bq_0+r_0=bq_1+r_1$ with $0\leq r_0,r_1<b$ and then show that $q_0=q_1$ and $r_0=r_1$.

B. Verify the statement for $a=0$. Show that if it holds when $a>0$ then it holds when $a<0$.

C. Prove the statement for $a>0$. *Hint:* note that the set $\{a-bq \bigm| q\in\mathbb{Z}\}$ has nonnegative elements, apply the Least Number Principle to get a smallest one, and show that it is the desired r.

Observe that the Division Theorem only covers the case where the divisor is positive. Observe also that $r=0$ if and only if $b\mid a$.

1.19 Definition. Where $m>0$, the remainder when a is divided by m is the *modulus* $a \bmod m$. Two numbers a,b are *congruent modulo* m, written $a\equiv c \pmod{m}$, if they leave the same remainder when divided by m, that is, if they have the same modulus with respect to m.

1.20 Exercise. Prove or disprove: (i) $a \bmod b = b \bmod a$ (ii) $a \bmod b = -a \bmod b$

1.21 Exercise. Prove that $a\equiv b \pmod{m}$ if and only if $m\mid(a-b)$, that is, if and only if a and b differ by a multiple of m, where $m>0$.

1.22 Exercise. Let a,b,c,d,m be integers with $m>0$, and $a\equiv b \pmod{m}$, and $c\equiv d \pmod{m}$. Prove each.

A. $a+c\equiv b+d \pmod{m}$

B. $ac\equiv bd \pmod{m}$

C. $a^n\equiv b^n \pmod{m}$ for all $n\in\mathbb{Z}^+$

1.23 Definition. For any real number x, its *floor* $\lfloor x\rfloor$ is the greatest integer less than or equal to x.

1.24 Exercise. Prove each.

A. The quotient when a is divided by b is $\lfloor a/b\rfloor$.

B. $a=b\cdot\lfloor a/b\rfloor + a \bmod b$

C. $b\cdot(a \bmod m) = (ba) \bmod (bm)$

1.25 Exercise. (Pigeonhole Principle) Prove each.

A. For a finite list of real numbers, the maximum is at least as big as the average.

B. If you have $n>0$-many pigeonholes and more than n-many papers then at least one hole gets at least two papers.

COMMON DIVISORS AND COMMON MULTIPLES

1.26 DEFINITION. An integer is a *common divisor* of two others if it divides both of them. The *greatest common divisor* of two integers is the largest of their common divisors, except that we take the greatest common divisor of 0 and 0 to be 0. Write $\gcd(a,b)$ for the greatest common divisor.

1.27 EXERCISE. Prove.

A. (EXISTENCE) Any $a,b\in\mathbb{Z}$ have a greatest common divisor.

B. (COMMUTATIVITY) $\gcd(a,b)=\gcd(b,a)$

C. For any $a\in\mathbb{Z}$, both $\gcd(a,a)=|a|$ and $\gcd(a,0)=|a|$.

D. If d is a common divisor of a and b then so is $|d|$. Thus common divisors are limited to the interval from $-\gcd(a,b)$ to $\gcd(a,b)$.

E. $\gcd(a,b)=\gcd(|a|,|b|)$

F. If both numbers are nonzero then $0<\gcd(a,b)\leq\min(|a|,|b|)$. If either is zero then the greatest common divisor is the maximum of the absolute values.

1.28 DEFINITION. Two numbers are *relatively prime* or *coprime*, sometimes denoted $a\perp b$, if their greatest common divisor is 1.

1.29 DEFINITION. The *least common multiple* of two positive integers $\operatorname{lcm}(a,b)$ is the smallest positive integer that is a multiple of each.

1.30 EXERCISE. Prove each. (i) (EXISTENCE) Any two positive integers have a least common multiple. (ii) (COMMUTATIVITY) $\operatorname{lcm}(a,b)=\operatorname{lcm}(b,a)$.

1.31 EXERCISE. (EUCLID'S ALGORITHM) Prove that if $a=bq+r$ then $\gcd(a,b)=\gcd(b,r)$.

The algorithm associated with this result quickly finds the greatest common divisor for any $a,b\in\mathbb{Z}$ with $a\geq b>0$. For instance, to find $\gcd(803,154)$ divide the larger by the smaller $803=154\cdot5+33$ and then Euclid's result has that $\gcd(803,154)=\gcd(154,33)$. Iterate: since $154=33\cdot4+22$, Euclid gives that $\gcd(154,33)=\gcd(33,22)$. Continuing as though we hadn't noticed that the answer is 11, we get $33=22\cdot1+11$ and $\gcd(33,22)=\gcd(22,11)$. Finally, $22=11\cdot2+0$ gives that $\gcd(22,11)=11$. The remainder of 0 signals that the algorithm has finished, yielding $\gcd(803,154)=11$.

We can reverse this calculation. From $33=22\cdot1+11$ we can express the greatest common divisor 11 as a combination $11=1\cdot33-1\cdot22$. Next, the equation $154=33\cdot4+22$ lets us express the 11 as a combination $11=1\cdot33-1\cdot(154-4\cdot33)=-1\cdot154+5\cdot33$ of the pair 154, 33. Backing up still further, the equation $803=154\cdot5+33$ gives $11=-1\cdot154+5\cdot(803-5\cdot154)=5\cdot803-26\cdot154$, so we can express the greatest common divisor as a combination of our initial pair 803, 154.

1.32 DEFINITION. A number c is a *linear combination* of two others a and b if it has the form $c=a\cdot m+b\cdot n$ for some $m,n\in\mathbb{Z}$.

1.33 EXERCISE. Use Euclid's Algorithm to find the greatest common divisor, and then reverse that to express the greatest common divisor as a linear combination of the two. (i) 123, 54 (ii) 48, 732

1.34 EXERCISE. Prove.

A. The greatest common divisors of two numbers is a linear combination of the two.

B. (BÉZOUT'S LEMMA) The greatest common divisor of two numbers is the smallest positive number that is a linear combination of the two. *Hint:* consider all linear combinations.

1.35 EXERCISE. You are given three buckets. The first two are marked 6 liters and 11 liters while the last one, which is quite large, is unmarked. Taking water from a nearby pond, use those buckets to end with 8 liters in the unmarked one.

1.36 EXERCISE. Let $a,b\in\mathbb{Z}$ and $m\in\mathbb{N}$. Prove each.

A. $\gcd(ma,mb)=m\cdot\gcd(a,b)$

B. If d is a common divisor of a and b then $\gcd(a/d,\,b/d)=\gcd(a,b)/d$. (From this it follows that if a and b are nonzero then $a/gcd(a,b)$ and $b/\gcd(a,b)$ are relatively prime.)

C. (EUCLID'S LEMMA) If a and b are relatively prime then $a\mid bc$ implies that $a\mid c$.

PRIMES

1.37 DEFINITION. An integer greater than 1 is *prime* if its only positive divisors are 1 and itself. A number greater than 1 that is not prime is *composite*.

1.38 EXERCISE. Verify each. (i) There are 25 primes less than 100. (ii) Below 50 there are 6 pairs of *twin primes*, primes separated by 2. (iii) The numbers $2^{2^0}+1,\ldots,2^{2^4}+1$ are prime.

1.39 EXERCISE. Prove.

A. An integer $n>1$ is composite if and only if it has two factors $n=a\cdot b$ (they may be equal) such that $1<a,b<n$.

B. Every number greater than 1 has a prime divisor.

C. Every composite number $n>1$ has a prime divisor p with $p\leq\sqrt{n}$. This inequality cannot be made strict.

1.40 EXERCISE. (EUCLID'S THEOREM) There are infinitely many primes.

1.41 EXERCISE. Suppose that p is a prime. Prove each.

A. If $p\mid ab$ then either $p\mid a$ or $p\mid b$.

B. If $p\mid a_0\cdot a_1\cdots a_{n-1}$ then p divides at least one a_i.

1.42 EXERCISE. (FUNDAMENTAL THEOREM OF ARITHMETIC) Any number $n>1$ can be expressed as a product of primes $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ and this expression is unique: if $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ and the primes are in ascending order $p_1<p_2<\cdots<p_k$ then any other factorization into a product of primes in ascending order will give the same result. We prove this in two parts.

A. Prove that any $n>1$ can be written as a product of one or more primes.

B. Prove that the factorization is unique. *Hint:* you can suppose that there are two factorizations into primes $n=p_0\cdots p_{s-1}$ and $n=q_0\cdots q_{t-1}$ in ascending order and use induction on s.

Remark: this result is why we do not include 1 among the primes. Including 1 would require us to change the clause about uniqueness since we can always multiply by additional 1's.

1.43 EXERCISE. Decide if each is true. (i) $5\cdot7\cdot19\neq3\cdot11\cdot17$ (ii) $1357\cdot4183=1081\cdot5251$

1.44 EXERCISE. Let $a,b>1$ and suppose that $a=p_0^{e_0}\cdots p_{n-1}^{e_{n-1}}$ and $b=p_0^{f_0}\cdots p_{n-1}^{f_{n-1}}$ are their prime factorizations (to use the same primes $p_0,\ldots,p_{n-1}$ in both we allow here that some exponents are zero). Prove that in the prime factorization of $\gcd(a,b)$ the exponent of p_i is $\min(\{e_i,f_i\})$. (Much the same proof shows that in the prime factorization of $\operatorname{lcm}(a,b)$ the exponent of p_i is $\max(\{e_i,f_i\})$. Taken together the two show that $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=ab$.)

1.45 EXERCISE. (EXISTENCE OF IRRATIONAL NUMBERS)

A. Prove that if a number is a square then in its prime factorization each prime is raised to an even power.

B. Prove that $\sqrt{2}$ is irrational.

Chapter 2 Sets

2.1 Definition. A *set* is a collection that is definite — every object either definitely is contained in the collection or definitely is not. An object x that belongs to a set A is an *element* or *member* of the set, written $x \in A$ (to denote that x is not an element of A write $x \notin A$). Two sets are equal if and only if they have the same elements.

Read '$\in$' as "is an element of" rather than "in" to avoid confusion between this and the subset relation defined below. As a synonym for set we sometimes say "collection."

We usually specify a set either by listing or by describing its elements. Thus we may write the set of the primes less than ten either as $P = \{2,3,5,7\}$ or as $P = \{p \in \mathbb{N} \mid p \text{ is prime and } p < 10\}$ (read the vertical bar as "such that"; some authors use a colon ':' instead of a vertical bar).

2.2 Exercise. Decide if each is true and justify your decision. (i) $\{1,3,5\} = \{5,3,1\}$ (ii) $\{2,4,6\} = \{2,4,6,4\}$ (iii) $\{1,3\} = \{n \in \mathbb{N} \mid n < 5\}$ (iv) $0 \in \{1,2,\{0\}\}$ (v) $4 \in \{n \in \mathbb{N} \mid n^2 < 50\}$

2.3 Definition. The set B is a *subset* of the set A if every element of B is an element of A, that is, provided that $x \in B$ implies that $x \in A$. We write $B \subseteq A$.

2.4 Definition. The set without any elements is the *empty set* $\varnothing$.

2.5 Exercise. Decide each, with justification. (i) $\{1,3,5\} \subseteq \{1,3,5,7,9\}$ (ii) $\{1,3,5\} \in \{1,3,5,7,9\}$ (iii) $\{1,3,5\} \subseteq \{n \in \mathbb{N} \mid n \text{ is prime}\}$ (iv) $\varnothing \subseteq \{1,2,3,4\}$ (v) $\{2\} \in \{1,\{2\},3\}$ (vi) $\{2\} \subseteq \{1,\{2\},3\}$

2.6 Exercise. Prove.

A. For all sets A, both $A \subseteq A$ and $\varnothing \subseteq A$

B. The empty set is unique: if the set A is empty and the set B is empty then $A = B$.

2.7 Exercise. Prove, for any sets A, B, and C.

A. (Mutual Inclusion) If $A \subseteq B$ and $B \subseteq A$ then $A = B$.

B. (Transitivity) If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

2.8 Exercise. For each, give an example of three sets satisfying the conditions, or show that no example is possible. (i) $A \subseteq B$, $B \not\subseteq C$, $A \subseteq C$ (ii) $A \not\subseteq B$, $B \not\subseteq C$, $A \subseteq C$ (iii) $A \not\subseteq B$ $B \subseteq C$, $A \subseteq C$

In this book statements talk about things inside of some *universal set*, denoted Ω. For instance, in the first chapter on number theory the universal set is the integers $\Omega = \mathbb{Z}$. There, if we say that we are considering the set of things less than 100 then we are considering the set of integers less than 100.

2.9 Definition. The *characteristic function* of a set A is a map χ_A (or $\mathbb{1}_A$), whose domain is the universal set, such that $\chi_A(x) = 1$ if $x \in A$, and $\chi_A(x) = 0$ if $x \notin A$.

2.10 Exercise. (Russell's Paradox) The definition that we gave allows sets to contain anything. This turns out to be naive. For, if sets can contain anything then we naturally think of the set that contains everything, all sets. Note that it contains itself as an element. In this way we are led to the set of all sets that don't contain themselves $D = \{S \mid S \notin S\}$.

A. Show that assuming D is an element of itself leads to a contradiction.

B. Show that assuming D is not an element of itself also leads to a contradiction.

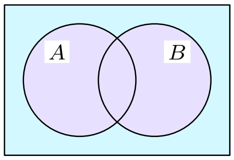
Operations

2.11 Definition. The *complement* of a set A, denoted A^{c}, is the set of objects that are not elements of A.

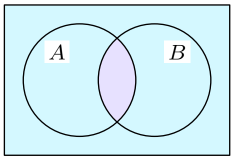
Remark: working inside of a universal set makes the complement operation sensible. For instance, in a number theory discussion where $\Omega = \mathbb{Z}$, if we consider the set of things less than 100 then we can take the complement and the result is another subset of Ω, so we are still in number theory.

2.12 Definition. Let A and B be sets. Their *union* is the collection of elements from either set, $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$. Their *intersection* is the collection of elements from both sets, $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

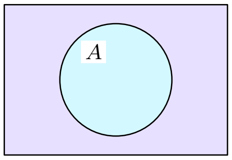
Picture set operations with *Venn diagrams.*



$A \cup B$



$A \cap B$



A^{c}

In each diagram the region inside the rectangle depicts the universal set and the region inside each circle depicts the set. On the left the darker color shows the union as containing all of the two sets joined, the middle shows the intersection containing only the region common to both, and on the right the dark region, the complement, is all but the set A.

2.13 Exercise. Another tool illustrating set relationships is this table describing two sets.

$x \in A$	$x \in B$	row number
0	0	0
0	1	1
1	0	2
1	1	3

We use 0 and 1 instead of F and T so that each row is the binary representation of its row number. That table gives $A = \{2,3\}$, $B = \{1,3\}$, and $\Omega = \{0,1,2,3\}$. For each of these simple results about set operations, apply the statement to the sets A and B. Also pick one and prove it. (i) the complement of the complement is the original set $(A^{\mathsf{c}})^{\mathsf{c}} = A$ (ii) $A \cap \varnothing = \varnothing$ and $A \cup \varnothing = A$ (iii) (Idempotence) $A \cap A = A$ and $A \cup A = A$ (iv) $A \cap B \subseteq A \subseteq A \cup B$ (v) (Commutativity) $A \cap B = B \cap A$ and $A \cup B = B \cup A$ (vi) (Associativity) $(A \cap B) \cap C = A \cap (B \cap C)$ and $(A \cup B) \cup C = A \cup (B \cup C)$

2.14 Exercise. Prove that the following are equivalent: (i) $A \subseteq B$, (ii) $A \cup B = B$, and (iii) $A \cap B = A$.

2.15 Definition. The *difference* of two sets is $A - B = \{x \in A \mid x \notin B\}$. The *symmetric difference* is $A \triangle B = (A - B) \cup (B - A)$.

If $A \subseteq X$ then $X - A$ is the same as A^{c} where X is the universal set $\Omega = X$.

2.16 Exercise. Prove or disprove

A. For any two sets, $A - B = A \cap B^{\mathsf{c}}$ (and thus $A - B \subseteq A$).

B. For all pairs of sets, $A - B = B - A$.

C. For all pairs of sets, $A \triangle B = B \triangle A$.

2.17 Exercise. (De Morgan's Laws) Prove, for all sets A, B, and C.

A. $(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$ and $(A \cup B)^{\mathsf{c}} = A^{\mathsf{c}} \cap B^{\mathsf{c}}$

B. (Distributivity) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

2.18 Definition. Two sets are *disjoint* if their intersection is empty.

2.19 Exercise. Find three sets A, B, and C, such that $A \cap B \cap C$ is empty but the sets are not pairwise disjoint, that is, none of $A \cap B$, $A \cap C$, or $B \cap C$ is empty.

2.20 Definition. For a finite set A, the *order* $|A|$ is the number of elements.

2.21 DEFINITION. For a set A the *power set* $\mathscr{P}(A)$ is the set of all subsets of A.

2.22 EXERCISE. List the elements of each power set $\mathscr{P}(\{0,1\})$, $\mathscr{P}(\{0,1,2\})$, $\mathscr{P}(\{0\})$, and $\mathscr{P}(\varnothing)$. Find the order of each.

2.23 EXERCISE. Let $A=\{\varnothing,\{\varnothing\}\}$. Decide, and justify, whether each is true or false. (i) $\varnothing\in\mathscr{P}(A)$, $\varnothing\subseteq\mathscr{P}(A)$ (ii) $\{\varnothing\}\in\mathscr{P}(A)$, $\{\varnothing\}\subseteq\mathscr{P}(A)$ (iii) $\{\{\varnothing\}\}\in\mathscr{P}(A)$, $\{\{\varnothing\}\}\subseteq\mathscr{P}(A)$

2.24 EXERCISE. Prove or disprove: if $A\subseteq B$ then $\mathscr{P}(A)\subseteq\mathscr{P}(B)$.

2.25 EXERCISE. Where A is a finite set, prove that $|\mathscr{P}(A)|=2^{|A|}$.

CARTESIAN PRODUCT

2.26 DEFINITION. A *sequence* $\langle x_0,x_1,\ldots,x_{n-1}\rangle$ is an ordered list of its *terms* x_0, x_1, ..., x_{n-1}. Its *length* $\operatorname{lh}(\langle x_0,x_1,\ldots,x_{n-1}\rangle)$ is the number of terms n. Two sequences are equal if and only if they have the same length and the same terms, in the same order.

2.27 EXERCISE. Prove or disprove. (i) $\langle 3,4,5\rangle=\langle 4,3,5\rangle$ (ii) $\langle 3,4,4,5\rangle=\langle 3,4,5\rangle$

2.28 DEFINITION. For sets A_0, A_1, ..., A_{n-1} the *Cartesian product* is the set of all length n sequences $A_0\times A_1\times\cdots\times A_{n-1}=\{\langle a_0,a_1,\ldots,a_{n-1}\rangle \bigm| a_0\in A_0,\ldots,\text{ and } a_{n-1}\in A_{n-1}\}$. We write A^n for for the Cartesian product of n equal sets $A\times\cdots\times A$.

Note the distinction between the diamond brackets $\langle\cdots\rangle$ that denote sequences and the curly braces $\{\cdots\}$ for sets. A sequence of length two is often called an *ordered pair* and written with parentheses (x_0,x_1) (similarly we have ordered triples, four-tuples, etc.). Thus we may write $\mathbb{R}^2=\{(x,y)\bigm| x,y\in\mathbb{R}\}$ for the Cartesian plane.

2.29 EXERCISE. Prove that $\mathbb{N}^2\subseteq\mathbb{Z}^2$. Generalize.

2.30 EXERCISE. (ALGEBRA OF CARTESIAN PRODUCT)

A. Prove that $A\times B=\varnothing$ iff $A=\varnothing$ or $B=\varnothing$.

B. Show that there are sets so that $A\times B\neq B\times A$. Under what circumstances is $A\times B=B\times A$?

C. Show that this statement is false: $A\times B\subseteq\hat{A}\times\hat{B}$ if and only if $A\subseteq\hat{A}$ and $B\subseteq\hat{B}$. Patch the statement to make it true.

2.31 EXERCISE. (INTERACTION OF CARTESIAN PRODUCT WITH OTHER SET OPERATIONS)

A. Prove that $(A\cup B)\times C=(A\times C)\cup(B\times C)$. What is the interaction of Cartesian product and intersection?

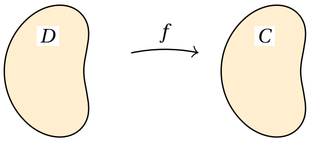
B. Show that in general $(A\times B)^{\mathsf{c}}$ does not equal $A^{\mathsf{c}}\times B^{\mathsf{c}}$.

CHAPTER 3 FUNCTIONS AND RELATIONS

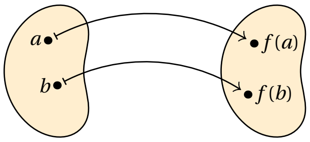
3.1 DEFINITION. A *function* f (or *map* or *morphism*) from *domain* set D to *codomain* set C, written $f\colon D \to C$, is a sequence consisting of the two sets along with a *graph*, a set of pairs $(d,c) \in D \times C$. This graph must be *well-defined*: for each $d \in D$ there is exactly one $c \in C$ such that (d,c) is an element of the graph. Functions are equal only if they have the same domain, codomain, and graph.

Thus, a function associates each element d from the domain, called an *argument* or *input*, with an element c from the codomain, called a *value* or *output*, subject to the condition that d determines c. We write $f(d) = c$ or $d \mapsto c$ and say that c is the *image* of d or that d *maps to* c.

A *bean diagram* pictures sets as blobs and either shows the entire function as a simple arrow, or else shows the function's action on individual elements with arrows that begin with a bar.



$f\colon D \to C$



$a \longmapsto f(a)$ and $b \longmapsto f(b)$

3.2 EXERCISE. Decide if each is a function. (i) $D = \{0,1,2\}$, $C = \{3,4,5\}$, $G = \{(0,3),(1,4),(2,5)\}$ (ii) $D = \{0,1,2\}$, $C = \{3,4,5\}$, $G = \{(0,3),(1,4),(2,3)\}$ (iii) $D = \{0,1,2\}$, $C = \{3,4,5\}$, $G = \{(0,3),(1,4)\}$ (iv) $D = \{0,1,2\}$, $C = \mathbb{N}$, $G = \{(0,3),(1,3),(2,3)\}$ (v) $D = \mathbb{N}$, $C = \mathbb{N}$, $G = \{(0,3),(1,4),(2,5)\}$ (vi) $D = \{0,1,2\}$, $C = \{3,4,5\}$, $G = \{(0,3),(1,4),(2,4),(0,5)\}$ (vii) $D = \mathbb{N}$, $C = \mathbb{N}$, $G = \{(d,c) \in D \times C \mid c = d^2\}$

Do not think that a function must have a formula. The final item in the prior exercise has a formula but for other items G just consists of arbitrary pairings.

3.3 EXERCISE. The *hailstone function* $h\colon \mathbb{N} \to \mathbb{N}$ is defined by cases,

$$h(n) = \begin{cases} n/2 & \text{– if } n \text{ is even} \\ 3n+1 & \text{– otherwise} \end{cases}$$

using a different formula when the input is even than when it is odd. (i) Compute $h(n)$ for $n = 0$, ..., $n = 9$. (ii) Starting with $n = 6$ iterate the function, that is, compute $h(n)$, then $h(h(n))$, etc., until the result is 1. How many steps does it take? (iii) How many steps does it take starting with $n = 11$? (The *Collatz conjecture* is that for every natural number starting value, iteration will eventually reach 1. No one knows if it is true.)

We are often not careful about the distinction between a function and its graph. For instance we may say, "a function is an input-output relationship" when technically it is the function's graph that is the pairing. (The distinction between function and graph is there only because the graph does not determine the codomain and so we must specify it separately. The graph does, however, determine the domain.)

In the edge case that the domain is the empty set, the only function possible is the empty set of ordered pairs.

3.4 EXERCISE. Show that $\{\langle q,n\rangle \in \mathbb{Q}^+ \times \mathbb{Z}^+ \mid n \text{ is } q\text{'s numerator}\}$ is not the graph of a function.

3.5 EXERCISE. When D and C are finite sets, how many functions are there from D to C?

A function may have multiple arguments; one example is the function $f\colon \mathbb{R}^2 \to \mathbb{R}$ whose action is $\langle x,y\rangle \mapsto x^2 - 2y^2$. We typically write $f(x,y)$ rather than $f(\langle x,y\rangle)$. We say this f is a 2-*ary* function (similarly there are 3-ary functions, etc.); the number of arguments is the function's *arity*.

3.6 DEFINITION. The *range* of $f\colon D \to C$ is $\operatorname{Ran}(f) = \{y \in C \mid \text{there is an } x \in D \text{ such that } f(x) = y\}$ (it is also denoted $f(D)$).

3.7 Exercise. For each item in Exericse 3.2, if it is a function then find its range.

3.8 Definition. Let $f\colon D\to C$. The *restriction* of f to $B\subseteq D$ is the function $f\restriction_B\colon B\to C$ whose action is given by $f\restriction_B(b)=f(b)$ for all $b\in B$ (we also say that f is an *extension* of $f\restriction_B$). The *image* of the set B under f, denoted $\operatorname{Im}(f)$ (or $f(B)$), is the range of the function $f\restriction_B$. In the other direction, the *inverse image of the element* $c\in C$ is the set $f^{-1}(c)=\{d\in D \mid f(d)=c\}$, and the *inverse image of the set* $A\subseteq C$ is $f^{-1}(A)=\{d\in D \mid f(d)\in A\}$.

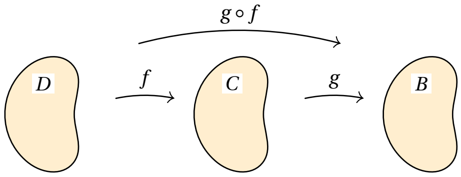
Observe that $f^{-1}(c)$ is a set, not an element.

3.9 Exercise. Where $f\colon\mathbb{R}-\{(2n+1)\pi/2 \mid n\in\mathbb{Z}\}\to\mathbb{R}$ is the function $f(x)=\tan(x)$, (i) find the image under f of the interval $[\pi/4\,..\,\pi/2)=\{x\in\mathbb{R} \mid \pi/4\le x<\pi/2\}$ (ii) find the image of the set $\{-\pi/3\}$ (iii) find the inverse image of the number 1.

3.10 Exercise. Prove that $f^{-1}(A)$ is the union of the sets $f^{-1}(a)$ over all $a\in A$.

Composition

3.11 Definition. The *composition* of two functions $f\colon D\to C$ and $g\colon C\to B$ is $g\circ f\colon D\to B$ given by $g\circ f(d)=g(f(d))$.



Read $g\circ f$ aloud as "g circle f" or as "g composed with f" (or "g following f"). Note that while in the expression $g\circ f$ the g is read first, the function that is applied first is f. Note also that the codomain of f is the domain of g (we sometimes allow a composition when the domain of g is not the entire codomain of f but instead is a superset of its range).

3.12 Exercise. Let $D=\{0,1,2\}$, $C=\{a,b,c,d\}$, and $B=\{\alpha,\beta,\gamma\}$ (these letters are not variables, they are distinct set elements). Let $f\colon D\to C$ be given by $0\longmapsto a$, $1\longmapsto c$, $2\longmapsto d$ and let $g\colon C\to B$ be given by $a\longmapsto\alpha$, $b\longmapsto\beta$, $c\longmapsto\gamma$, and $d\longmapsto\alpha$. (i) Compute $g\circ f$ on all arguments or show that the composition is not defined. (ii) Compute $f\circ g$ on all arguments or show that it is not defined. (iii) Find the range of f, g, and any defined compositions

3.13 Exercise. Let $f\colon\mathbb{R}\to\mathbb{R}$ be $f(x)=x^2$ and let $g\colon\mathbb{R}\to\mathbb{R}$ be $g(x)=3x+1$. Find the domain, codomain, and a formula for $g\circ f$ and $f\circ g$.

3.14 Exercise. Prove each. (i) (Associativity) $h\circ(g\circ f)=(h\circ g)\circ f$ (ii) Function composition need not be commutative.

Inverse

The definition of a function specifies that for every input there is exactly one associated output. This is asymmetric because the definition puts no such condition on elements of the codomain.

3.15 Definition. A function is *one-to-one* (or an *injection*) if for each value there is at most one associated argument, that is, if $f(d_0)=f(d_1)$ implies that $d_0=d_1$ for all elements d_0,d_1 of the domain. A function is *onto* (or a *surjection*) if for each value there is at least one associated argument, that is, if for each element c of the codomain there exists an element d of the domain such that $f(d)=c$. A function that is both one-to-one and onto, so that for every value there is exactly one associated argument, is a *correspondence* (or *bijection*, or *permutation*).

3.16 Exercise. Let $f\colon\mathbb{R}\to\mathbb{R}$ be $f(x)=3x+1$ and $g\colon\mathbb{R}\to\mathbb{R}$ be $g(x)=x^2+1$.

A. Show that f is one-to-one, and onto.

B. Show that g is not one-to-one, and not onto.

3.17 EXERCISE. Let D and C be finite sets. Prove that if there is a correspondence $f\colon D \to C$ then the two have the same number of elements. We do this in two parts, each of which is useful on its own.

A. If f is one-to-one then $|C| \geq |D|$.

B. If f is onto then $|C| \leq |D|$.

3.18 EXERCISE. Prove.

A. A composition of one-to-one functions is one-to-one.

B. A composition of onto functions is onto. (With the prior item this gives that a composition of correspondences is a correspondence.)

C. If $g \circ f$ is onto then g is onto.

D. If $g \circ f$ is one-to-one then f is one-to-one.

E. Do the other two cases hold?

3.19 DEFINITION. An *identity function* $\mathrm{id}\colon D \to D$ has the action $\mathrm{id}(d) = d$ for all $d \in D$.

3.20 DEFINITION. Given $f\colon D \to C$, if $g \circ f$ is the identity function then g is a *left inverse* function of f, or what is the same thing, f is a *right inverse* of g. If g is both a left and right inverse of f then it is an *inverse* (or a *two-sided inverse*) of f, denoted f^{-1}.

3.21 EXERCISE. Show each.

A. Let $g\colon \mathbb{R}^3 \to \mathbb{R}^2$ be the projection $(x,y,z) \mapsto (x,y)$ and let $f\colon \mathbb{R}^2 \to \mathbb{R}^3$ be the injection $(x,y) \mapsto (x,y,0)$. Then g is a left inverse of f but not a right inverse.

B. The function $f\colon \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n^2$ has no left inverse function.

C. Where $D = \{0,1,2,3\}$ and $C = \{\alpha,\beta\}$, the function $f\colon D \to C$ given by $0 \mapsto \alpha$, $1 \mapsto \beta$, $2 \mapsto \alpha$, $3 \mapsto \beta$ has more than one right inverse.

3.22 EXERCISE. Compute each. (i) Where $f\colon \mathbb{Z} \to \mathbb{Z}$ is $f(a) = a+3$ and $g\colon \mathbb{Z} \to \mathbb{Z}$ is $g(a) = a-3$, show that g is inverse to f. (ii) Where $h\colon \mathbb{Z} \to \mathbb{Z}$ is the function that returns $n+1$ if n is even and returns $n-1$ if n is odd, find a function inverse to h. (iii) If $s\colon \mathbb{R}^+ \to \mathbb{R}^+$ is $s(x) = x^2$, find s's inverse.

3.23 EXERCISE. Let $D = \{0,1,2\}$ and $C = \{\alpha,\beta,\gamma\}$. Also let $f,g\colon D \to C$ be given by $f(0) = \alpha$, $f(1) = \beta$, $f(2) = \gamma$, and $g(0) = \alpha$, $g(1) = \alpha$, $g(2) = \gamma$. Then: (i) verify that f is a correspondence (ii) construct an inverse for f (iii) verify that g is not a correspondence (iv) show that g has no inverse.

In Definition 3.8, we defined $f^{-1}(c)$ to be the set $\{d \in D \mid f(d) = c\}$. While this earlier notation is standard, it conflicts what we just saw in Definition 3.20. For instance, if $g\colon \mathbb{R} \to \mathbb{R}$ is $g(x) = 2x$ then $g^{-1}(8)$ could mean two things: the earlier definition has $g^{-1}(8) = \{4\}$ while the above definition has $g^{-1}(8) = 4$. However, the difference between the one-element set and the single element isn't very big and doesn't cause much trouble. The way that trouble can arise happens with $\hat{g}\colon \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$. The earlier definition has $\hat{g}^{-1}(9) = \{3,-3\}$. As to the above, though, the function is not invertible and so $\hat{g}^{-1}(9)$ is not defined.

In short, if a function f has an inverse then the distinction between the two definitions is minor. But if f has no inverse then the earlier definition still applies; put another way, the use of the symbol f^{-1} in the earlier definition does not imply that the function has an inverse.

3.24 EXERCISE. Prove.

A. A function has an inverse if and only if that function is a correspondence.

B. If a function has an inverse then that inverse is unique.

C. The inverse of a correspondence is a correspondence.

D. If f and g are each invertible then so is $g \circ f$, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Relations

A function's graph is a set of pairs, subject to the condition that the input determines the output. We next generalize functions by dropping that condition.

3.25 Definition. A *relation* on sets $A_0, \ldots, A_{n-1}$ is a subset $R \subseteq A_0 \times \cdots \times A_{n-1}$. If all of the sets are the same $A_0 = A_1 = \cdots = A$ then we say it is a relation on A. If $n = 2$ then it is a *binary relation.* In this case, where $\langle a_0, a_1 \rangle \in R$ we say that a_0 is R*-related* to a_1, sometimes written $a_0 R a_1$. For larger n we say R is n*-ary*, and call n the *arity* of the relation

3.26 Exercise. List five elements of each relation: (i) $\{\langle x, y \rangle \in \mathbb{N}^2 \mid x \text{ and } y \text{ have the same parity}\}$ (recall that numbers have the same parity if they are both even or both odd) (ii) less-than <, as a binary relation on $\mathbb{N}$ (iii) $\{\langle x, y, z \rangle \in \mathbb{N}^3 \mid x^2 + y^2 = z^2\}$ (iv) the relation $E = \{(x, y) \in A \times \mathscr{P}(A) \mid x \in y\}$ where $A = \{0, 1, 2\}$.

3.27 Exercise. For any function $f\colon D \to C$, verify that $R_f = \{(x, y) \in D^2 \mid f(x) = f(y)\}$ is a binary relation. List five elements of R_f. when $f(x) = x^2$, with domain and codomain $\mathbb{R}$.

3.28 Definition. Let R be a binary relation on a set X. The relation is *reflexive* if $\langle x, x \rangle \in R$ for all $x \in X$. The relation is *symmetric* if $\langle x, y \rangle \in R$ implies that $\langle y, x \rangle \in R$ for all $x, y \in R$. The relation is *transitive* if $\langle x, y \rangle \in R$ and $\langle y, z \rangle \in R$ implies that $\langle x, z \rangle \in R$ for all elements $x, y, z \in R$. A relation that satisfies all three conditions is an *equivalence relation.*

3.29 Exercise. For each of the three conditions reflexive, symmetric, or transitive, prove or disprove that the relation satisfies the condition.

A. The "goes into" relation $D = \{\langle d, m \rangle \in \mathbb{Z}^2 \mid d \mid m\}$.

B. For any set A the *diagonal relation* on A is $\{\langle a, a \rangle \mid a \in A\}$.

C. The relation on $\mathbb{R}$ of 'at least two greater' $T = \{\langle x, y \rangle \in \mathbb{R}^2 \mid x - y \geq 2\}$.

3.30 Exercise. Fix a divisor $m \in \mathbb{Z}^+$. Show that the relation $\{\langle a, b \rangle \in \mathbb{Z}^2 \mid a \equiv b \pmod{m}\}$ is an equivalence.

3.31 Exercise. Let $\mathscr{L}$ be the set of lines in the Euclidean plane and consider the relation $R = \{\langle \ell_0, \ell_1 \rangle \in \mathscr{L}^2 \mid \text{the two are parallel or are equal}\}$. (i) List five elements of R. (ii) Where ℓ is a vertical line, list five elements of $\mathscr{L}$ that are related to ℓ. (iii) Show that R is an equivalence.

3.32 Exercise. A binary relation on $A = \{0, 1\}$ is a set of pairs $\langle a_0, a_1 \rangle$ where $a_0, a_1 \in A$. There are sixteen such relations. Characterize each as reflexive or not, symmetric or not, and transitive or not.

3.33 Exercise. Relations can be reflexive or not, symmetric or not, and transitive or not, so there are eight possible combinations.

A. Four of the combinations are not reflexive (e.g., one is: not reflexive, not symmetric, and not transitive). For each, give an example relation on $A = \{0, 1, 2\}$.

B. Give examples of binary relations on $A = \{0, 1, 2\}$ for the other four combinations.

3.34 Exercise. Let elements $\langle p, q \rangle$ and $\langle n, d \rangle$ of $\mathbb{Z} \times \mathbb{Z}^+$ be related if $pd = qn$. That is, consider the relation $\{(\langle p, q \rangle, \langle n, d \rangle) \in (\mathbb{Z} \times \mathbb{Z}^+)^2 \mid pd = qn\}$. List five elements. Prove that it is an equivalence.

3.35 Definition. If R is an equivalence relation on X then we sometimes write $x \equiv y \pmod{R}$ instead of $\langle x, y \rangle \in R$. The *equivalence class* of $x \in X$ is the set $[\![x]\!] = \{y \in X \mid y \equiv x \pmod{R}\}$.

A common stumbling block is that $[\![x_0]\!] = [\![x_1]\!]$ does not imply that $x_0 = x_1$. One example is the relation of leaving the same remainder when divided by ten, $R = \{\langle x, y \rangle \in \mathbb{N}^2 \mid 10 \mid (x - y)\}$. The set of numbers that leave a remainder of 1 is $\{1, 11, 21, 31, \ldots\}$ and this set can be identified as the equivalence class of 1, or the equivalence class of 11, etc.: $[\![1]\!] = [\![11]\!] = [\![21]\!] = \cdots$.

3.36 Exercise. Verify that each relation is an equivalence on X. Exhibit the equivalence classes.

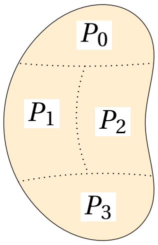
A. $x_0 \equiv x_1 \pmod{R}$ if they have the same parity (are both even or both odd), with $X = \mathbb{N}$

B. $i \equiv n \pmod{R}$ if $i \equiv n \pmod{3}$ (they leave the same remainder on division by 3), with $X = \mathbb{Z}$

C. $x_0 \equiv x_1 \pmod{R}$ if $x_0 - x_1 \in \mathbb{Z}$, with $X = \mathbb{R}$

3.37 EXERCISE. Let R be an equivalence on X. Prove that the following are equivalent statements for $x_0, x_1 \in X$: (i) $x_0 \equiv x_1 \pmod{R}$ (ii) $[\![x_0]\!] = [\![x_1]\!]$ and (iii) $[\![x_0]\!] \cap [\![x_1]\!] \neq \varnothing$.

3.38 DEFINITION. A *partition* $\mathcal{P}$ of a set X is a collection of nonempty subsets of $P \subseteq X$ such that every element $x \in X$ is in exactly one of the P's. That is, $\mathcal{P}$ partitions X if and only if each $P \in \mathcal{P}$ is nonempty, and $\mathcal{P}$ *covers* X (the union of all $P \in \mathcal{P}$ is equal to X), and the P are *pairwise disjoint* (if $P \cap \hat{P} \neq \varnothing$ then $P = \hat{P}$).



Set X partitioned into four subset parts $\mathcal{P} = \{P_0, P_1, P_2, P_3\}$

3.39 EXERCISE. Verify that $\mathcal{P}$ is a partition of X. How many elements are in $\mathcal{P}$?

A. $X = \mathbb{N}$, $\mathcal{P} = \{P_0, P_1\}$, where P_0 is the set of even numbers and P_1 is the set of odd numbers.

B. $X = \mathbb{Z}$, $\mathcal{P} = \{P_n \mid n \in \mathbb{Z}\}$ where $P_n = \{i \in \mathbb{Z} \mid i \equiv n \pmod{3}\}$

C. $X = \mathbb{R}$, $\mathcal{P} = \{P_x \mid x \in \mathbb{R}\}$ where $P_x = \{y \in \mathbb{R} \mid x - y \in \mathbb{Z}\}$

3.40 EXERCISE. Prove.

A. Where R is an equivalence on the set X, the collection of equivalence classes $\{[\![x]\!] \mid x \in X\}$ forms a partition of X, the partition *induced* by the relation.

B. Where $\mathcal{P}$ is a partition of X, the relation $R = \{\langle x, y\rangle \in X^2 \mid x \text{ and } y \text{ are in the same part}\}$ is an equivalence, the relation that *arises from* the partition.

3.41 EXERCISE. Suppose $f \colon D \to C$.

A. Show that the relation $R = \{(d_0, d_1) \in D^2 \mid f(d_0) = f(d_1)\}$ is an equivalence on D.

B. Prove that the set of inverse images $\mathcal{P} = \{f^{-1}(c) \mid c \in \operatorname{Ran}(f)\}$ partitions the domain.

C. Consider the map $\hat{f} \colon \mathcal{P} \to \operatorname{Ran}(f)$ whose action is: $\hat{f}(P)$ is defined to be $f(d)$ where $d \in P$. Show that $\hat{f}$ is a function and that it is one-to-one. *Remark:* every function can be modified to be onto by changing its codomain to equal its range. This exercise gets one-to-one-ness by modifying the function's domain.

3.42 DEFINITION. A binary relation R is *antisymmetric* if $\langle x, y\rangle \in R$ and $\langle y, x\rangle \in R$ implies that $x = y$. A binary relation is a *partial ordering* if it is reflexive, antisymmetric, and transitive.

3.43 EXERCISE. Verify each.

A. The usual less than or equal to relation $\leq$ on the real numbers is a partial order.

B. The relation 'divides' on $\mathbb{N}$ is a partial order.

C. For any set A the relation $\subseteq$ on $\mathscr{P}(A)$ is a partial order.

3.44 EXERCISE. Can a relation be both symmetric and antisymmetric?

CHAPTER 4 INFINITY

Recall Exercise 3.17, that if two finite sets correspond then they have the same number of elements.

4.1 DEFINITION. Two sets have the *same cardinality* (or are *equinumerous*) if there is a correspondence from one to the other. We write $A \sim B$.

4.2 DEFINITION. A set is *finite* if it has n elements for some $n \in \mathbb{N}$, that is, if it has the same cardinality as $\{i \in \mathbb{N} \bigm| i < n\} = \{0, 1, \ldots, n-1\}$. Otherwise the set is *infinite*. A set is *denumerable* if it has the same cardinality as $\mathbb{N}$. A set is *countable* if it is either finite or denumerable.

4.3 EXERCISE. Prove that the relation $\sim$ is an equivalence.

4.4 EXERCISE. Prove.

A. The set of integers is countable.

B. The set $\mathbb{N} \times \mathbb{N}$ is countable.

4.5 EXERCISE. Prove that the following are equivalent for a set A: (i) A is countable (ii) A is empty or there is an onto function from $\mathbb{N}$ to A (iii) there is a one-to-one function from A to $\mathbb{N}$.

4.6 EXERCISE. Prove that the set of rational numbers is countable.

4.7 EXERCISE. Prove that each of these infinite sets is not countable.

A. $\mathscr{P}(\mathbb{N})$

B. $\mathbb{R}$

Appendix: Peano axioms

Particularly in the first chapter a person struggles with when to consider a statement sufficiently justified and soon comes to wonder what the axioms are like. Here we give the most often used axiom system for the natural numbers, to convey a sense of that.

This system was introduced by Dedekind in 1888 and tuned by Peano in 1889. In addition to the usual logical and set symbols such as = and $\in$, with the traditional properties, our language will use at least two symbols, 0 and S, whose properties are limited by the conditions below.

Axiom. (Existence of a natural number) The constant 0 is a natural number.

Axiom. (Arithmetical properties) The *successor* function S has these properties.

a. (Closure) For all $a \in \mathbb{N}$, its successor $S(a)$ is also a natural number.

b. (One-to-one) For all $a, b \in \mathbb{N}$, if $S(a) = S(b)$ then $a = b$.

c. (Almost onto) For all $a \in \mathbb{N}$, if $a \neq 0$ then there is a $b \in \mathbb{N}$ with $S(b) = a$. In contrast, no $c \in \mathbb{N}$ has 0 as a successor.

These properties give infinitely many natural numbers: 0, $S(0)$, $S(S(0))$, etc. Of course, the notation 0, 1, 2, etc., is less clunky.

Axiom. (Induction) Suppose that K is a set satisfying both (i) $0 \in K$ and (ii) for all $n \in \mathbb{N}$, if $n \in K$ then $S(n) \in K$. Then $K = \mathbb{N}$.

In this book we use an induction variant that changes condition (ii) to: for all $k \in \mathbb{N}$, if $n \in K$ for $0 \leq n \leq k$ then $S(k) \in K$. Condition (ii) above is often called *weak induction* while the version we use is *strong induction.* There are technical differences but for our purposes the two variants are interchangeable. We prefer the strong variant because while it is more awkward to state, it is sometimes easier to apply.

From those axioms we can for instance define addition by recursion using successor

$$\operatorname{add}(a,n) = \begin{cases} a & \text{if } n = 0 \\ S(\operatorname{add}(a,m)) & \text{if } n = S(m) \end{cases}$$

and then define multiplication by recursion using addition.

$$\operatorname{mul}(a,n) = \begin{cases} 0 & \text{if } n = 0 \\ \operatorname{add}(\operatorname{mul}(a,m),a) & \text{if } n = S(m) \end{cases}$$