An Inquiry-Based

INTRODUCTION TO PROOFS

Jim Hefferon
Saint Michael's College
Version 2.0

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
$\lvert A \rvert$	cardinality 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
$\mathrm{id}\colon D \to D$	identity map, defined by $\mathrm{id}(d) = d$
$f\restriction_B$	restriction of f to a subset of its domain
$f^{-1}(c)$, $f^{-1}(A)$	inverse image of an element or of a subset of the codomain
$g \circ f$	function composition
f^{-1}	the 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

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 proof writing for majors in Mathematics.

APPROACH. This course is Inquiry-Based, sometimes called the Discovery Method (an older term is Moore Method). Students get a sequence of things to prove, along with definitions and a few remarks. They attempt these outside of class, and then in class they propose solutions, and carefully examine the solutions proposed by others. The instructor only lightly guides and the students pledge not to use outside sources. Together, they talk through misunderstandings, sometimes stumble in the dark, and sometimes have beautiful flashes of insight. In short, they *do* the mathematics.

There are two advantages. First, students own it — they are completely engaged. This is the ultimate in active learning. Second, through their discussions, students come not only to see what is right but also to understand why what's wrong is wrong. For these students, with this material, this is the best way to develop mathematical maturity. Besides, it is a lot of fun.

For more, see the book's web site described below, and the site of Communities for Mathematics Inquiry in Teaching Network.

TOPICS. The only prerequisite is high school mathematics. In a semester, I cover the first three chapters, on elementary number theory, sets, functions, and relations.

We start with number theory instead of sets for the same reason that the baseball team's practice starts with tossing the ball and not with reading the rule book. 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 get on board quickly. The second and third chapters cover what they will need for later classes, keeping the intellectual habits that we've established at the start.

EXERCISES. To the extent possible, nearby exercises have about the same difficulty. This level 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 and in class I ask a different student to propose a solution for each. If the labels are i, ii, etc., then a single person does them all.

ACKNOWLEDGMENTS. The material is standard but I must recognize my debt to the wonderful presentations of J Jensen-Vallin and D Velleman. I am also glad for the chance to thank the students of past classes in Proofs, who have taught me a great deal.

WEB SITE. This book is Free. In particular, you are free to copy it and distribute those copies. See this book's page at `hefferon.net/proofs`. That page has a version of this text that fits on seven double-sided sheets, which you can just hand out on the first day. That's what I do.

It has other material that you may find useful, including some classroom slides and a handout for students about the basics of writing mathematics. All of it comes with the LaTeX source, so that you can adapt it to your needs.

I am always glad to get reports, either a description of your experience, or suggestions, or bugs. Please email me at the address on the web site.

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

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

Jim Hefferon
Saint Michael's College,
Colchester, Vermont USA
2021-Summer

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, d *goes evenly into* n, n *is divisible by* d, or n *is a multiple of* d.) We write $d \mid n$ if d is a divisor of n, or $d \nmid n$ if it is not.

1.2 Definition. A number is *even* if it is divisible by 2, otherwise it is *odd*. (We may instead say that the *parity* is even or odd.)

The notation $d \mid n$ signifies a relationship between two integers. 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) Each of these is a statement about integers. Prove each.

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 both $-d \mid a$ and $d \mid -a$. In addition, d divides $|a|$ (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. That is, for each decide if it is true or false and if it is true then prove it, while if it is false then give a counterexample.

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

1.5 Exercise. Generalize the first item of the prior exercise to be a statement about sums of multiples of $d \in \mathbb{Z}$, and then prove your statement.

1.6 Exercise. (Interaction of parity and multiplication) Prove or disprove. (i) The product of two evens is even. (ii) The quotient of two evens, if it is an integer, is even.

1.7 Exercise. For the prior exercise's first item, formulate and prove a generalization that applies to any integer.

1.8 Exercise. (Divisibility properties) Prove each. Assume that all the numbers are integers.

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) Where $d, n \in \mathbb{Z}$, if there is a nonzero integer a such that $ad \mid an$ then $d \mid n$. And, 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 and -1. The only numbers that divide 1 are 1 and -1.

G. The largest divisor of any nonzero $a \in \mathbb{Z}$ is $|a|$.

H. Every nonzero integer has only finitely many divisors.

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

1.10 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) This generalizes the prior item: if $a \mid b$ and $a \mid c$ then a divides $m \cdot b + n \cdot c$ for any $m, n \in \mathbb{Z}$.

INTERLUDE: INDUCTION

The results in the prior section need only proof techniques that many people find come naturally. However some results to follow require a technique that is less natural, mathematical induction. This section introduces it. (We will start with exercises about summations. However, note that induction is not about only summation. They just make good starting exercises.)

For example, many people have, in playing with numbers, 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, and 1, etc., gives a family of statements: $S(0)$, and $S(1)$, 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 initial number $i \in \mathbb{N}$ (sometimes there is a finite list of initial numbers). The *inductive step* is more subtle; we show that the following implication holds.

> If the statement holds from the initial number or numbers through the $n=k$ case, then the statement holds also in the next case, where $n=k+1$. (∗)

The *Principle of Mathematical Induction* is that proving both the base and inductive steps shows that the statement is true for all natural numbers greater than or equal to the initial number.

For the intuition behind that principle, consider again the statement about odds and squares. The base step directly verifies the statement for the initial number, 0. Then, because 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 $S(0)$, 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 natural numbers.

Here is the full proof that $1+3+5+\cdots+(2n+1)=(n+1)^2$ for all $n \in \mathbb{N}$.

Proof. We will show this by induction. For the $n=0$ base step, 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 the $n=0$, $n=1$, ..., $n=k$ cases, and consider the $n=k+1$ case. The sum is $1+3+\cdots+(2k+1)+\big(2(k+1)+1\big)=1+3+\cdots+(2k+1)+(2k+3)$. The inductive hypothesis is that 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 value for the $n=k+1$ case. ∎

1.11 EXERCISE. Prove by induction.

A. $0+1+2+3+\cdots+n=n(n+1)/2$

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

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

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

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

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

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

1.14 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 $n=2$ for the base step.

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

1.15 EXERCISE. Prove that 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.

Many induction arguments use only the $n=k$ part of the hypothesis but some use other parts.

1.16 EXERCISE. The game of Nim starts with two piles, each with n chips. The two players take turns picking a pile, and taking from it a nonzero number of chips. The player taking the final chip wins. Prove by induction on n that this is a winning strategy for player two: whatever number of chips that player one takes from a pile, player two takes the same number from the other pile.

1.17 EXERCISE. The *Fibonacci sequence* $0,1,1,2,3,5,8,13,\ldots$ satisfies that each number is the sum of the prior two, $f_n = f_{n-1} + f_{n-2}$, along with $f_0 = 0$ and $f_1 = 1$. The following argument purports to show that all Fibonacci numbers are even; where is it wrong? "First, 0 is even. For the inductive step, assume the statement holds for all cases up to and including $n = k$. Then the next number f_{k+1} is the sum of the two prior numbers, which by the inductive hypothesis are both even."

1.18 DEFINITION. The *Well-Ordering Principle*, or *Least Number Principle*, is that any nonempty subset of the natural numbers has a least element.

1.19 EXERCISE. Prove each.

A. The Principle of Induction implies the Well-Ordering Principle. *Hint:* use induction on $n \in \mathbb{N}$ to show that if a set of natural numbers contains n then it has a least element.

B. The Well-Ordering Principle, along with the observation that every nonzero natural number has a predecessor, implies the Principle of Induction. *Hint:* consider a set that contains 0, and having the property that if it contains $0,\ldots k$ then it contains $k+1$. Show this set must equal $\mathbb{N}$.

DIVISION

1.20 EXERCISE. (EUCLIDEAN DIVISION) For any integers a, b with $b \neq 0$ there are unique integers q, r such that $a = bq + r$ and $0 \leq r < |b|$. Here, a is the *dividend* and b is the *divisor*, while q is the *quotient* and r is the *remainder*. We prove this in three steps.

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 deduce that $q_0 = q_1$ and $r_0 = r_1$.

B. Verify that there exists such a q, r pair when $a = 0$. Show that if the statement holds when $a > 0$ then it holds when $a < 0$.

C. Prove the statement for $a > 0$. *Hint:* show that the set $\{a - bq \mid q \in \mathbb{Z}\}$ has nonnegative elements, apply the Least Number Principle to get a smallest one r, and verify that this has the properties required of a remainder.

1.21 DEFINITION. Where $m \neq 0$, the remainder when a is divided by m is the *modulus*, a mod 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.

1.22 EXERCISE. Find (i) 5 mod 3, (ii) -5 mod 3. (iii) 5 mod -3, (iv) -5 mod -3.

1.23 EXERCISE. Prove or disprove: (i) a mod $b = b$ mod a, (ii) a mod $b = -a$ mod b

1.24 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 $m \neq 0$.

Remark: many authors define $a \equiv b \pmod{m}$ with $m \mid (a - b)$, and impose that $m > 1$.

1.25 EXERCISE. Suppose $a, b, c, d, m \in \mathbb{Z}$, and $m \neq 0$, and $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$. Prove each.

A. $a \equiv b \pmod{m}$ if and only if $a \equiv b \pmod{-m}$

B. $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

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

1.26 DEFINITION. For $x \in \mathbb{R}$, the *floor*, $\lfloor x \rfloor$, is the greatest integer less than or equal to x. The *ceiling*, $\lceil x \rceil$, is the least integer greater than or equal to x.

1.27 EXERCISE. Prove each, where $a, b, c \in \mathbb{Z}$ and $b \neq 0$.

A. The quotient when a is divided by b is: $\lfloor a/b \rfloor$ for $b > 0$, and $\lceil a/b \rceil$ for $b < 0$.

B. $c \cdot (a \bmod b) = (ca) \bmod (cb)$

COMMON DIVISORS AND COMMON MULTIPLES

1.28 DEFINITION. A *common divisor* of $a, b \in \mathbb{Z}$ is an integer that divides both. Where at least one of them is nonzero, their *greatest common divisor*, $\gcd(a,b)$, is the largest of their common divisors.

1.29 EXERCISE. Prove.

A. (EXISTENCE) For any two integers a, b that are not both zero, $\gcd(a,b)$ exists and is positive.

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

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

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

E. If both numbers are nonzero then $0 < \gcd(a,b) \leq \min(|a|,|b|)$. If one number is zero and the other is not then the greatest common divisor is the absolute value of the other.

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

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

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

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

The algorithm associated with this result finds greatest common divisors quickly. For instance, to find $\gcd(803,154)$, divide the larger by the smaller $803 = 154 \cdot 5 + 33$ and then the prior result gives that $\gcd(803,154) = \gcd(154,33)$. Iterate: from $154 = 33 \cdot 4 + 22$, we have that $\gcd(154,33) = \gcd(33,22)$. Continuing gives $33 = 22 \cdot 1 + 11$ and $\gcd(33,22) = \gcd(22,11)$, and the last step is that $22 = 11 \cdot 2 + 0$ shows that $\gcd(22,11) = 11$. The zero remainder signals that we are done, and we conclude that $\gcd(803,154) = 11$.

Reversing this calculation is also useful. Start by rewriting $33 = 22 \cdot 1 + 11$ to put the greatest common divisor on the left, $11 = 1 \cdot 33 - 1 \cdot 22$. Next, rewrite the next equation $154 = 33 \cdot 4 + 22$ to isolate its remainder and substitute: $11 = 1 \cdot 33 - 1 \cdot (154 - 4 \cdot 33) = -1 \cdot 154 + 5 \cdot 33$. Finally, from $803 = 154 \cdot 5 + 33$ we $11 = -1 \cdot 154 + 5 \cdot (803 - 5 \cdot 154) = 5 \cdot 803 - 26 \cdot 154$. This expresses the greatest common divisor 11 as a combination of the initial numbers 803 and 154.

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

1.35 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

1.36 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 the set of all combinations.

1.37 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.

1.38 EXERCISE. Prove each, for $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}$.

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

B. If $a, b \in \mathbb{Z}$ are not both zero, and d is a common divisor, then $\gcd(a/d, b/d) = \gcd(a,b)/d$. Thus, $a/gcd(a,b)$ 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

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

1.40 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.

1.41 EXERCISE. Prove.

A. A number n is composite if and only if it decomposes into the product of two factors, $n = a \cdot b$, which are greater than 1 and less than n (the two might be equal).

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

C. Every composite number n has a prime divisor p that is less than or equal to $\sqrt{n}$. This inequality cannot be made strict.

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

1.43 EXERCISE. Let p be prime. Prove each.

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

B. If $p \mid a_0 \cdot a_1 \cdots a_{n-1}$ for $n \geq 2$ then p divides at least one a_i.

1.44 EXERCISE. (FUNDAMENTAL THEOREM OF ARITHMETIC) Any number $n > 1$ decomposes into a product of primes, $n = p_0^{e_0} p_1^{e_1} \cdots p_s^{e_s}$. This factgorization is unique: if the primes are in ascending order, $p_0 < p_1 < \cdots p_s$, and if each exponent is nontrivial, $e_i > 0$, then any two prime factorizations have the same primes with the same exponents. We prove this in two parts.

A. Prove that any number greater than 1 can be written as a product of primes.

B. Prove that the factorization is unique. *Hint:* show that where $n = p_0 \cdots p_i$ is a product of (possibly not distinct) primes and if $n = q_0 \cdots q_j$ is also a product of primes, then the primes are the same, with the same multiplicities, possibly rearranged. You can use induction on i.

Remark: this result is why we do not include 1 among the primes. If we called 1 a prime then we would have to change the uniqueness clause, since we can always multiply by additional 1's.

1.45 EXERCISE. True or false? (i) $5 \cdot 7 \cdot 19 = 3 \cdot 11 \cdot 17$ (ii) $1357 \cdot 4183 = 1081 \cdot 5251$

1.46 EXERCISE. Let $a = p_0^{e_0} \cdots p_n^{e_n}$ and $b = p_0^{f_0} \cdots p_n^{f_n}$ express each as a product of unequal primes; to use the same list of primes $p_0, \ldots, p_n$ for both, we allow here that some exponents are zero. Prove that the prime factorization of $\gcd(a,b)$ is $p_0^{g_0} \cdots p_n^{g_n}$, where $g_i = \min(\{e_i, f_i\})$. (Much the same argument shows that in the prime factorization of $\operatorname{lcm}(a,b)$, the exponent of p_i is $\max(\{e_i, f_i\})$. Together these show that $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.)

1.47 EXERCISE. (EXISTENCE OF IRRATIONAL NUMBERS)

A. Prove that in the prime factorization of a square, each prime is raised to an even power.

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

CHAPTER 2 SETS

A *set* is a collection. (Our sets will only contain mathematical objects, such as numbers.) An object x that belongs to a set A is an *element* or *member* of that set, denoted $x \in A$. To denote that x is not an element, use $x \notin A$. Sets are equal if and only if they have the same elements.

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

2.1 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) $4 \in \{n \in \mathbb{N} \mid n^2 < 50\}$ (v) $0 \in \{1,2,\{0\}\}$

2.2 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 $B \subseteq A$.

2.3 DEFINITION. The set without any elements is the *empty set*, denoted $\varnothing$.

2.4 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) $\{2\} \subseteq \{1,\{2\},3\}$

2.5 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 $A = B$.

2.6 EXERCISE. Prove, for 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 $A \subseteq C$.

Remark: the most common way to show that two sets are equal is through mutual inclusion.

2.7 EXERCISE. For each, give an example of three sets satisfying the conditions, or show that no example is possible. (i) $A \subseteq B$, $B \nsubseteq C$, $A \subseteq C$ (ii) $A \nsubseteq B$, $B \nsubseteq C$, $A \subseteq C$ (iii) $A \nsubseteq B$ $B \subseteq C$, $A \subseteq C$

Usually mathematical statements are made in the context of some *universe*, denoted Ω. For instance, in the first chapter the universe is the set of 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. Another example is that in first semester calculus, the universe is the set of real numbers, $\Omega = \mathbb{R}$.

2.8 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 is the collection of all sets. Note that this set contains itself. In this way, we are led to consider the 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.

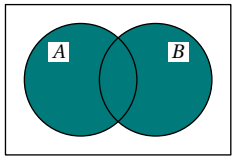
SET OPERATIONS

2.9 DEFINITION. The *complement* of a set A, denoted A^{c} (or $\overline{A}$), is the set of things that are not elements of A.

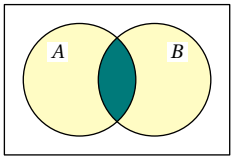
Remark: working inside of a universe makes the complement sensible. For instance, in a number theory discussion where $\Omega = \mathbb{Z}$, if we consider the set $A = \{m \in \mathbb{Z} \mid m < 100\}$, then taking the complement, $A^{\mathsf{c}} = \{m \in \mathbb{Z} \mid m \geq 100\}$, yields another subset of Ω, so we are still in number theory.

2.10 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, $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

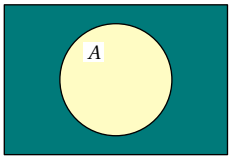
Picture set operations with *Venn diagrams*.



$A \cup B$



$A \cap B$

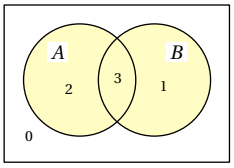


A^{c}

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

2.11 EXERCISE. Another tool for illustrating set relationships is this table. It is convenient for systematically covering the cases involving the universe $\Omega = \{0,1,2,3\}$, along with the two sets $A = \{2,3\}$ and $B = \{1,3\}$. (It uses 0 and 1 in place of F and T so that the right side of each row is the binary representation of its number.)

Number x	$x \in A$	$x \in B$
0	0	0
1	0	1
2	1	0
3	1	1



The table's top row says that $0 \notin A$ and $0 \notin B$, while the second row says that $1 \notin A$ but $1 \in B$. For each of these simple results about set operations, apply the statement to these example sets. Also, pick one statement 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 $(A \cup B) \cup C = A \cup (B \cup C)$ (extend the table to add a third set, C).

2.12 EXERCISE. Prove that the following statements are equivalent: (i) $A \subseteq B$, (ii) $A \cup B = B$, and (iii) $A \cap B = A$. *Hint:* one approach is to show that (i) implies (ii), that (ii) implies (iii), and that (iii) implies (i).

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

Remark: the complement of a set is the difference between the universe and the set, $A^{\mathsf{c}} = \Omega - A$.

2.14 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, $A \triangle B = B \triangle A$.

2.15 EXERCISE. Prove, for all sets A, B, and C.

A. (DE MORGAN'S LAWS) $(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$ 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 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

2.16 DEFINITION. Two sets are *disjoint* if their intersection is empty.

2.17 EXERCISE. Find three sets A, B, and C, such that the triple $A \cap B \cap C$ is empty but the three pairs $A \cap B$, $A \cap C$, and $B \cap C$, are all nonempty.

2.18 DEFINITION. For a finite set A, the *cardinality*, $|A|$, is the number of elements.

2.19 EXERCISE. For finite sets, if $A \subseteq B$ then $|A| \leq |B|$.

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

2.21 EXERCISE. List the elements of each power set, and also state the cardinality of each: (i) $\mathscr{P}(\{0,1\})$, (ii) $\mathscr{P}(\{0,1,2\})$, (iii) $\mathscr{P}(\{0\})$, and (iv) $\mathscr{P}(\varnothing)$.

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

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

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

CARTESIAN PRODUCT

2.25 DEFINITION. A *sequence* $\langle x_0, x_1, \ldots x_{n-1} \rangle$ is an ordered list. Its elements x_0, x_1, $\ldots$ x_{n-1} are *terms*. Its *length* $\mathrm{lh}(\langle x_0, x_1, \ldots x_{n-1} \rangle)$ 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.

2.26 EXERCISE. True or false? (i) $\langle 1,3,5 \rangle = \langle 5,3,1 \rangle$ (ii) $\langle 2,4,6 \rangle = \langle 2,4,6,4 \rangle$

2.27 DEFINITION. For sets A_0, A_1, $\ldots$ A_{n-1}, where $a_0 \in A_0$, $a_1 \in A_1$, $\ldots$ $a_{n-1} \in A_{n-1}$, the collection of all sequences $\langle a_0, a_1, \ldots a_{n-1} \rangle$ is the *Cartesian product*, denoted $A_0 \times A_1 \times \cdots \times A_{n-1}$. If the sets are equal then we write $A^n = A \times \cdots \times A$.

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 $\mathbb{R}^2 = \{(x,y) \;\big|\; x, y \in \mathbb{R}\}$ for the Cartesian plane.

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

2.29 EXERCISE. (ALGEBRA OF CARTESIAN PRODUCT)

A. Prove that $A \times B = \varnothing$ if and only if $A = \varnothing$ or $B = \varnothing$.

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

C. Show that this 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 it to make it true.

2.30 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 about intersection?

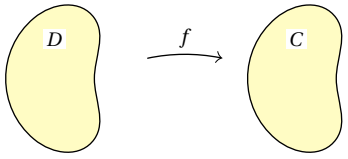
B. Show that in general $(A \times B)^{\mathsf{c}}$ does not equal $A^{\mathsf{c}} \times B^{\mathsf{c}}$.

Chapter 3 Functions and relations

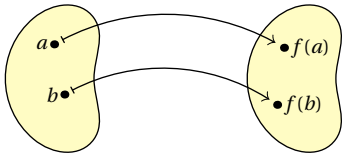
3.1 Definition. A *function* or *map* f from *domain* set D to *codomain* set C, written $f\colon D \to C$, is a triple consisting of the two sets along with a *graph*, a set of pairs $(d,c) \in D \times C$. The function must be *well-defined*: for each $d \in D$ there must be exactly one $c \in C$ such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

That is, 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*, with 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 the graph is most reasonably understood as just arbitrary pairs.

3.3 Exercise. The *hailstone function* $h\colon \mathbb{N} \to \mathbb{N}$ is defined by cases: if n is even then $h(n) = n/2$, and otherwise $h(n) = 3n+1$. (i) Compute $h(n)$ for $n = 0, \ldots, n = 9$. (ii) Iterate the function starting with input 6, that is, compute $h(6)$, then $h(h(6))$, 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 starting value greater than zero, iteration will eventually reach 1. No one knows if it is true.)

We often blur the distinction between a function and its graph. We may say, "a function is an input-output relationship" when actually the function's graph is the pairing. (We distinguish between a function and its graph only because the graph does not determine the codomain, so we must specify that separately. The graph does, however, determine the domain.)

Where the domain or codomain is empty, the only possible function has an empty graph. This is called the *empty function*.

3.4 Exercise. Show that $\{\langle x,y\rangle \in \mathbb{R}^2 \mid y^2 = x\}$ 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?

3.6 Definition. The *characteristic function* of a set A is a map χ_A (some authors write $\mathbb{1}_A$), from the universe Ω to the set $\{0,1\}$, such that $\chi_A(x) = 1$ if $x \in A$ and $\chi_A(x) = 0$ if $x \notin A$.

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 write $f(x,y)$ rather than $f(\langle x,y\rangle)$. We say that this f is 2-*ary* and similarly there are 3-ary functions, etc. The number of arguments is the function's *arity*.

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

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

3.9 Definition. Let $f\colon D \to C$. The *restriction* of f to the subset $B \subseteq D$ is the function $f\restriction_B\colon B \to C$ 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

subset B, denoted $\mathrm{Im}(f)$ or $f(B)$, is the range of $f\restriction_B$. 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 $f^{-1}(A) = \{d \in D \mid f(d) \in A\}$.

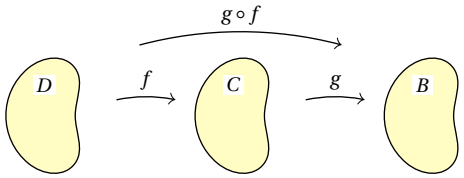
Observe that $f^{-1}(c)$ is a set, not an element.

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

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

COMPOSITION

3.12 DEFINITION. The *composition* of two functions $f : D \to C$ and $g : C \to B$ is $g \circ f : D \to B$, given by $g \circ f\,(d) = g(f(d))$.



Read $g \circ f$ aloud as "g composed with f" or "g circle f." Note that there is an awkwardness about the expression $g \circ f$: while you read the g first, the function that you apply first is f. Note also that the domain of g is the codomain of f. We are often casual about this and don't object to a composition as long as the the range of f is a subset of the domain of g.

3.13 EXERCISE. Let $D = \{0,1,2\}$, $C = \{10,11,12,13\}$, and $B = \{20,21,22\}$. Let $f : D \to C$ be given by $0 \mapsto 10$, $1 \mapsto 12$, and $2 \mapsto 13$. Also let $g : C \to B$ be $10 \mapsto 20$, $11 \mapsto 21$, $12 \mapsto 22$, and $13 \mapsto 20$. (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 and g, as well as of $g \circ f$ and $f \circ g$, if they are defined.

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

3.15 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 function requires that for each input element there is one and only one associated output. There is an asymmetry here because it puts no such condition on output elements.

3.16 DEFINITION. A function $f : D \to C$ is *one-to-one*, or an *injection*, if for each member of the codomain there is at most one associated member of the domain, that is, for all $d_0, d_1 \in D$, the equality $f(d_0) = f(d_1)$ implies that $d_0 = d_1$. The function is *onto*, or a *surjection*, if for each member of the codomain there is at least one associated domain member, that is, if for all $c \in C$ there is at least one $d \in D$ such that $f(d) = c$. A function that is both one-to-one and onto, so that for every member of the codomain there is one and only one associated domain member, is a *correspondence* or *bijection*.

3.17 EXERCISE. Let $f : \mathbb{R} \to \mathbb{R}$ be $f(x) = 3x + 1$ and $g : \mathbb{R} \to \mathbb{R}$ 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.

3.18 EXERCISE. Prove these for a function f with a finite domain D. They imply that corresponding finite sets have the same size. *Hint:* for each, you can do induction on either $|D|$ or $|\mathrm{Ran}(f)|$.

A. $|\mathrm{Ran}(f)| \leq |D|$

B. If f is one-to-one then $|\text{Ran}(f)| = |D|$.

3.19 EXERCISE. (PIGEONHOLE PRINCIPLE) Show that if $n > 0$-many pigeonholes contain a total of more than n-many papers, then at least one hole has at least two papers.

3.20 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 one-to-one then f is one-to-one.

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

E. If $g \circ f$ is onto, is f onto? If it is one-to-one, is g one-to-one?

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

3.22 DEFINITION. Given $f\colon D \to C$, if $g \circ f = \text{id}$ 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 *two-sided inverse*) of f, denoted f^{-1}.

3.23 EXERCISE. Show each.

A. Let $g\colon \mathbb{R}^3 \to \mathbb{R}^2$ be the projection $(x,y,z) \mapsto (x,y)$. 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.

C. Where $D = \{0,1,2,3\}$ and $C = \{10,11\}$, the function $f\colon D \to C$ given by $0 \mapsto 10$, $1 \mapsto 11$, $2 \mapsto 10$, $3 \mapsto 11$ has more than one right inverse.

3.24 EXERCISE. (i) Where $f\colon \mathbb{Z} \to \mathbb{Z}$ is $f(a) = a+3$, find a function inverse to f. Of course, you must verify that it is inverse. (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 an inverse.

3.25 EXERCISE. Let $D = \{0,1,2\}$ and $C = \{10,11,12\}$. Also let $f,g\colon D \to C$ be $f(0) = 10$, $f(1) = 11$, $f(2) = 12$, and $g(0) = 10$, $g(1) = 10$, $g(2) = 12$. 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 3.9, we wrote $f^{-1}(c)$ for the set $\{d \in D \mid f(d) = c\}$. This earlier notation is standard but it conflicts with what we just saw in Definition 3.22. 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 $g^{-1}(8) = 4$. The difference between the set containing one element and that one element doesn't cause much trouble. However, when the function is not one-to-one then we must be careful. For $\hat{g}\colon \mathbb{R} \to \mathbb{R}$ given by $\hat{g}(x) = x^2$, the earlier definition has $\hat{g}^{-1}(9) = \{3,-3\}$. But because $\hat{g}$ is not one-to-one, it is not invertible, and so $\hat{g}^{-1}$ in the sense of Definition 3.22 doesn't even exist.

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

3.26 EXERCISE. Prove.

A. A function has an inverse if and only if that it 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 ⟨argument, value⟩, subject to the condition that the argument determines the value. We now generalize by dropping that condition.

3.27 DEFINITION. A set of ordered pairs $R \subseteq A_0 \times A_1$ is a *binary relation*. Where $\langle a_0, a_1 \rangle \in R$, we say that a_0 is R-*related* to a_1, sometimes written $a_0 R a_1$. In general, a *relation* on sets $A_0, \ldots, A_{n-1}$ is a subset of the Cartesian product, $R \subseteq A_0 \times \cdots \times A_{n-1}$. If all of the sets are the same, $A_0 = A_1 = \cdots = A$, then we say it is a relation on A. We say that R is n-*ary*, and call n the *arity* of the relation.

3.28 EXERCISE. List five elements of each relation: (i) $\{\langle x, y \rangle \in \mathbb{N}^2 \mid x \text{ and } y \text{ have the same parity}\}$, (ii) less-than, $<$, as a binary relation on $\mathbb{Z}$, (iii) $\{\langle x, y, z \rangle \in \mathbb{N}^3 \mid x^2 + y^2 = z^2\}$, (iv) $E = \{(x, y) \in A \times \mathscr{P}(A) \mid x \in y\}$, where $A = \{0, 1, 2\}$.

3.29 EXERCISE. Verify that for any function $f : D \to C$, the set $R_f = \{(x, y) \in D^2 \mid f(x) = f(y)\}$ is a binary relation. Where $f : \mathbb{R} \to \mathbb{R}$ is the function $f(x) = x^2$, list six elements of R_f.

3.30 DEFINITION. Let R be a binary relation on a set X. It is *reflexive* if $\langle x, x \rangle \in R$ for all $x \in X$. It is *symmetric* if $\langle x, y \rangle \in R$ implies that $\langle y, x \rangle \in R$ for all $x, y \in X$. And, it is *transitive* if $\langle x, y \rangle \in R$ and $\langle y, z \rangle \in R$ imply that $\langle x, z \rangle \in R$, for $x, y, z \in X$. A relation that is all three is an *equivalence*.

3.31 EXERCISE. Decide if each is reflexive or not, symmetric or not, and transitive or not. Of course, you must prove your assertions.

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

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

C. The relation on the reals of "at least two greater," $T = \{\langle x, y \rangle \in \mathbb{R}^2 \mid x - y \geq 2\}$.

3.32 EXERCISE. Fix an integer $m \neq 0$. Show that $E_m = \{\langle a, b \rangle \in \mathbb{Z}^2 \mid a \equiv b \pmod{m}\}$ is an equivalence.

3.33 EXERCISE. Let $\mathscr{L}$ be the set of lines in the Euclidean plane and consider the relation $R = \{\langle \ell_0, \ell_1 \rangle \in \mathscr{L}^2 \mid \text{the two are parallel or equal}\}$. (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.

3.34 EXERCISE. There are sixteen binary relations on $A = \{0, 1\}$. List them and characterize each as reflexive or not, symmetric or not, and transitive or not.

3.35 EXERCISE. Binary relations can be reflexive or not, symmetric or not, and transitive or not, so there are eight possible combinations.

A. Give an example relation on $A = \{0, 1, 2\}$ for each of the four cases that are not reflexive.

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

3.36 EXERCISE. Let two elements $\langle n_0, d_0 \rangle$ and $\langle n_1, d_1 \rangle$ of $\mathbb{Z} \times \mathbb{Z}^+$ be related if $n_0 d_1 = d_0 n_1$. List five elements of this relation. Prove that it is an equivalence.

3.37 DEFINITION. If R is an equivalence relation on X then we usually write $x \equiv y \pmod{R}$, or $x \sim y$, in place of $\langle x, y \rangle \in R$. The *equivalence class* of $x \in X$ is the set $[\![x]\!] = \{y \in X \mid y \equiv x \pmod{R}\}$.

Note that $[\![x_0]\!] = [\![x_1]\!]$ does not imply that $x_0 = x_1$. An example is the relation of leaving the same remainder when divided by ten, $E_{10} = \{\langle x, y \rangle \in \mathbb{N}^2 \mid x \bmod 10 = y \bmod 10\}$. The set of numbers that leave a remainder of 1 is $\{1, 11, 21, 31 \ldots\}$ and we could identify this set as the equivalence class of 1, or the equivalence class of 11, etc.: $[\![1]\!] = [\![11]\!] = [\![21]\!] = \cdots$.

3.38 EXERCISE. Verify that each is an equivalence relation and exhibit the equivalence classes.

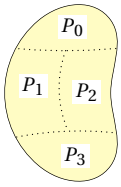
A. Two numbers $x_0, x_1 \in \mathbb{N}$ are related if they have the same parity.

B. Two natural numbers are related if they have the same leading digit (take the leading digit of zero to be 0).

C. Two real numbers $r_0, r_1 \in \mathbb{R}$ are related if $r_0 - r_1 \in \mathbb{Z}$.

3.39 EXERCISE. Let R be an equivalence relation 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) $[\![x_0]\!] \cap [\![x_1]\!] \neq \varnothing$.

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



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

3.41 EXERCISE. Verify that $\mathcal{P}$ is a partition of X. How many parts does it have?

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 $P_x = \{y \in \mathbb{R} \mid x - y \in \mathbb{Z}\}$

3.42 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. This is 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. This is the equivalence relation that *arises from* the partition.

3.43 EXERCISE. Let $f\colon D \to C$.

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

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

C. Using that partition, consider $\hat{f}\colon \mathcal{P} \to \text{Ran}(f)$ defined by: $\hat{f}(P) = f(d)$ for any $d \in P$. Show that $\hat{f}$ is well-defined and one-to-one. *Remark:* any function can be modified to be onto by setting its codomain to be its range. Here we also change the domain to get one-to-one.

3.44 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.

3.45 EXERCISE. Verify each.

A. The usual less than or equal to relation on the real numbers, $\leq$, 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.

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

Chapter 4 Infinity

Recall Exercise 3.18, that if two finite sets correspond then they have the same number of elements.

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

4.2 Exercise. For each, prove that the two have the same cardinality. (i) $\mathbb{N}$ and $E = \{2k \mid k \in \mathbb{N}\}$ (ii) $(-\pi/2 \,..\, \pi/2)$ and $\mathbb{R}$ (iii) $(0 \,..\, 1)$ and $\mathbb{R}$

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

4.4 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 some initial segment $\{i \in \mathbb{N} \mid i < n\} = \{0, 1, \ldots, n-1\}$ of the natural numbers. 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.

4.5 Exercise. Prove each.

A. The set of integers is countable.

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

4.6 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 $\mathbb{N}$.

4.7 Exercise. Prove that the set of rational numbers is countable.

4.8 Exercise. Prove that each of these infinite sets is not countable.

A. The power set of the naturals, $\mathscr{P}(\mathbb{N})$. *Hint:* suppose that $f : \mathscr{P}(\mathbb{N}) \to \mathbb{N}$ and consider $\{n \in \mathbb{N} \mid n \notin f(n)\}$.

B. The set of real numbers, $\mathbb{R}$. *Hint:* find a one-to-one map from $\mathscr{P}(\mathbb{N})$ to $\mathbb{R}$.

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

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

and then define multiplication by recursion using addition.

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