

An Inquiry-Based

INTRODUCTION TO PROOFS

Jim Hefferon
Saint Michael's College
Version 2.0

NOTATION

\mathbb{N}	natural numbers $\{0, 1, 2, \dots\}$
\mathbb{Z}, \mathbb{Z}^+	integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$, positive integers $\{1, 2, \dots\}$
\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
$\gcd(a, b), \text{lcm}(a, b)$	greatest common divisor, least common multiple
$a \in A$	a is an element of the set A
\emptyset	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
$A - B, A \Delta B$	difference, symmetric difference of the sets
$ A $	order of the set A ; the number of elements
$\mathcal{P}(A)$	power set of A ; the set of all of A 's subsets
$\langle x_0, x_1, \dots \rangle, (x_0, x_1)$	sequence, ordered pair
$\text{lh}(\langle x_0, x_1, \dots \rangle)$	length of the sequence
$A_0 \times A_1 \times \dots \times A_{n-1}, A^n$	Cartesian product of sets, product of a set with itself
$f: D \rightarrow C$	function with domain D and codomain C
$\text{id}: D \rightarrow D$	identity map; $\text{id}(d) = d$
$f \upharpoonright_B$	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 PRONUNCIATION

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

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

CHAPTER 1 NUMBERS

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

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 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*. (We may instead say that the *parity* is even or odd.)

The notation $d \mid n$ signifies a relationship between two integers. Note that 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.

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

- The sum of two evens is even. The difference of two evens is even.
- The sum of two odds is odd. The difference of two odds is odd.
- Where $a, b \in \mathbb{Z}$, the number $a + b$ is even if and only if $a - b$ is even.
- Generalize the first item to be a statement about sums of multiples of some $d \in \mathbb{Z}$. Prove it.

1.5 EXERCISE. (INTERACTION OF PARITY AND MULTIPLICATION) Prove or disprove.

- The product of two evens is even. Formulate and prove an analogous statement that applies to any integer.
- The quotient of two evens, if it is an integer, is even.

1.6 EXERCISE. (DIVISIBILITY PROPERTIES) Prove each. Assume that all the numbers are integers.

- (REFLEXIVITY) Every number divides itself.
- Every number divides 0 while the only number that 0 divides is itself.
- (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.
- (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 $a \in \mathbb{Z}$.
- (COMPARISON) For $d, n \in \mathbb{Z}^+$, if n is a multiple of d then $n \geq d$.
- Every number is divisible by 1 and -1 . The only numbers that divide 1 are 1 and -1 .
- The largest divisor of a is $|a|$, for $a \in \mathbb{Z}$ with $a \neq 0$.
- 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 $a, b, c \in \mathbb{Z}$.

- Prove that if $a \mid b$ then $a \mid bc$ for all integers c .
- Prove that if $a \mid b$ and $a \mid c$ then a divides the sum $b + c$ and difference $b - c$.
- (LINEARITY) Prove that 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

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 introduces induction. We will start with exercises about summations. (However, note that induction is not about summation; they just 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 statements: $S(0)$, 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 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.

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

The *Principle of Mathematical Induction* is that doing 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. (We sometimes instead use induction to show that a statement is true for all numbers in a finite interval.)

Here is an induction argument for the example statement.

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 $n = 0, n = 1, \dots, n = k$, 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 $a, b, r \in \mathbb{R}$ and that $r \neq 1$.

- A. (GEOMETRIC SERIES) $1 + r + r^2 + \cdots + r^n = (r^{n+1} - 1)/(r - 1)$
- B. (ARITHMETIC SERIES) $b + (a + b) + (2a + b) + \cdots + (na + b) = (n(n + 1)/2) \cdot a + (n + 1) \cdot b$

1.11 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 $n = 2$ for the base step.
- C. If $n \in \mathbb{Z}^+$ then $(1 + 1/n) \cdot (1 + 1/2) \cdots (1 + 1/n) = n + 1$.

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.

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

1.14 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 that by using this strategy the second player always wins: whatever number of chips the first player takes from one pile, the second player takes the same number from the other pile.

1.15 EXERCISE. The *Fibonacci number sequence* $0, 1, 1, 2, 3, 5, 8, 13, \dots$ satisfies that each succeeding number is the sum of the prior two $f_{n+1} = f_{n-1} + f_n$, with $f_0 = 0$ and $f_1 = 1$. The following argument purports to show that all Fibonacci numbers are even. Where does it go wrong? “The base step 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.”

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. Prove each.

- A. The Principle of Induction implies the Least Number 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 Least Number Principle implies the Principle of Induction. *Hint*: start with a set that contains 0 and such that if it contains $0, \dots, k$ then it contains $k + 1$, and show this set equals \mathbb{N} .

DIVISION

1.18 EXERCISE. (DIVISION THEOREM, OR DIVISION ALGORITHM) 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 the *dividend* and b is the *divisor*, while q is the *quotient* and r is the *remainder*. We prove this statement 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 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.

Observe 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 $a \equiv b \pmod{m}$, 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. Find (i) $5 \bmod 3$, (ii) $-5 \bmod 3$.

1.21 EXERCISE. Prove or disprove: (i) $a \bmod b = b \bmod a$, (ii) $a \bmod b = -a \bmod b$

1.22 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 $m > 0$.

1.23 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 powers $n \in \mathbb{Z}^+$

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

1.25 EXERCISE. Prove each, where $a, b, m \in \mathbb{Z}$ and $b > 0$.

- A. The quotient when a is divided by b is $\lfloor a/b \rfloor$. Thus, $a = b \cdot \lfloor a/b \rfloor + a \bmod b$.
- B. $b \cdot (a \bmod m) = (ba) \bmod (bm)$

COMMON DIVISORS AND COMMON MULTIPLES

1.26 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.

1.27 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 either number is zero then the greatest common divisor is the absolute value of the other.

1.28 DEFINITION. Two integers 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 $\text{lcm}(a, b)$ 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) $\text{lcm}(a, b) = \text{lcm}(b, a)$.

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 $a, b \in \mathbb{N}$. 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: since $154 = 33 \cdot 4 + 22$, 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 $\gcd(803, 154) = 11$.

Reversing this calculation is also fruitful. 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: $11 = 1 \cdot 33 - 1 \cdot (154 - 4 \cdot 33) = -1 \cdot 154 + 5 \cdot 33$. Similarly using $803 = 154 \cdot 5 + 33$ gives $11 = -1 \cdot 154 + 5 \cdot (803 - 5 \cdot 154) = 5 \cdot 803 - 26 \cdot 154$. This expresses the greatest common divisor 11 as a combination of the initial numbers 803 and 154.

1.32 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 the set of all 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. 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

1.37 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*.

1.38 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 $2^{2^0} + 1, \dots, 2^{2^4} + 1$ are prime.

1.39 EXERCISE. Prove.

- A. A number n is composite if and only if it can be decomposed into the product of two factors $n = a \cdot b$ such that $1 < a, b < n$ (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 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. 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 .

1.42 EXERCISE. (FUNDAMENTAL THEOREM OF ARITHMETIC) Any number $n > 1$ can be factored into primes, $n = p_0^{e_0} p_1^{e_1} \cdots p_s^{e_s}$. What's more, if the primes are distinct then this expression is unique: for each prime p_i , any two prime factorizations of n have the same power e_i of p_i . We prove this in two parts.

- A. Prove that any $n > 1$ 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, 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. Including 1 would require us to change the clause about uniqueness, since we can always multiply by additional 1's.

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

1.44 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 number as a product of distinct primes; to use the same primes p_0, \dots, p_n 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 $\text{lcm}(a, b)$ the exponent of p_i is $\max(\{e_i, f_i\})$. Together these show that $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.)

1.45 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 that is definite, so that every thing 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 that set, denoted $x \in A$. Denote that x is not an element with $x \notin A$. Sets are equal if and only if they have the same elements. (Read '∈' as "is an element of" rather than "in" to avoid confusion between this and the subset relation defined below.)

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

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 \emptyset .

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) $\emptyset \subseteq \{1, 2, 3, 4\}$ (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 $\emptyset \subseteq A$
- 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 $A \subseteq C$.

Mutual inclusion is the most common way to show that two sets are equal.

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

Usually mathematical statements are in a context of some *universe*, denoted Ω . For instance, in the first chapter the universe 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. 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 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.

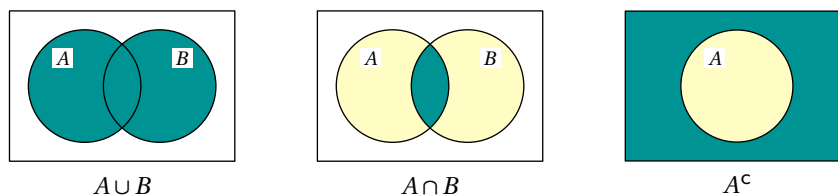
OPERATIONS

2.9 DEFINITION. The *complement* of a set A , denoted A^c , is the set of things that are not elements of A . Some authors denote the complement with a bar, \overline{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 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.

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

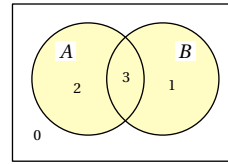
Picture set operations with *Venn diagrams*.



In each diagram the region inside the 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 illustrating set relationships is this table. It describes two sets in the universe $\Omega = \{0, 1, 2, 3\}$. (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	$x \in A$	$x \in B$
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 $(A^c)^c = A$ (ii) $A \cap \emptyset = \emptyset$ and $A \cup \emptyset = A$ (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 $A \Delta B = (A - B) \cup (B - A)$.

Remark: if $A \subseteq X$ then $X - A$ is the same as A^c where X is the universe, $\Omega = X$.

2.14 EXERCISE. Prove or disprove.

- For any two sets, $A - B = A \cap B^c$ (and thus $A - B \subseteq A$).
- For all pairs of sets, $A - B = B - A$.
- For all pairs of sets, $A \Delta B = B \Delta A$.

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

- (DE MORGAN'S LAWS) $(A \cap B)^c = A^c \cup B^c$ and $(A \cup B)^c = A^c \cap B^c$
- (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 $A \cap B \cap C$ is empty but the sets are not pairwise disjoint, that is, $A \cap B$, $A \cap C$, and $B \cap C$ are all nonempty.

2.18 DEFINITION. For a finite set A , the *order* $|A|$ 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* $\mathcal{P}(A)$ is the set of all subsets of A .

2.21 EXERCISE. List the elements of each power set: (i) $\mathcal{P}(\{0, 1\})$, (ii) $\mathcal{P}(\{0, 1, 2\})$, (iii) $\mathcal{P}(\{0\})$, and (iv) $\mathcal{P}(\emptyset)$. State the order of each.

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

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

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

CARTESIAN PRODUCT

2.25 DEFINITION. A *sequence* $\langle x_0, x_1, \dots, x_{n-1} \rangle$ is an ordered list. Its elements x_0, x_1, \dots, x_{n-1} are *terms*. Its *length* $\text{lh}(\langle x_0, x_1, \dots, x_{n-1} \rangle)$ 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, \dots, A_{n-1} , the collection of all sequences $\langle a_0, a_1, \dots, a_{n-1} \rangle$ where $a_0 \in A_0, a_1 \in A_1, \dots$, is the *Cartesian product*, denoted $A_0 \times A_1 \times \dots \times A_{n-1}$. If the sets are equal we write $A^n = A \times \dots \times A$.

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

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

2.29 EXERCISE. (ALGEBRA OF CARTESIAN PRODUCT)

- Prove that $A \times B = \emptyset$ iff $A = \emptyset$ or $B = \emptyset$.
- Show that there are sets so that $A \times B \neq B \times A$. Under what circumstances are they equal?
- 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)

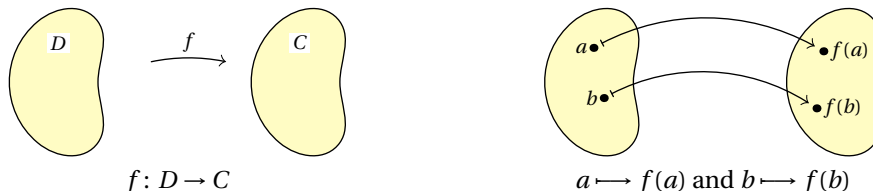
- Prove that $(A \cup B) \times C = (A \times C) \cup (B \times C)$. What about intersection?
- Show that in general $(A \times B)^c$ does not equal $A^c \times B^c$.

CHAPTER 3 FUNCTIONS AND RELATIONS

3.1 DEFINITION. A *function* or *map* f from *domain* set D to *codomain* set C , written $f: D \rightarrow C$, 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.

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.



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 G just has arbitrary pairings.

3.3 EXERCISE. The *hailstone function* $h: \mathbb{N} \rightarrow \mathbb{N}$ is defined by cases.

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

(i) Compute $h(n)$ for $n = 0, \dots, n = 9$. (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. 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 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 or codomain is empty, the only function has an empty graph.

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 $\mathbb{1}_A$), whose domain is the universe, 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 $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 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 $f: D \rightarrow C$ is $\text{Ran}(f) = \{y \in C \mid \text{there is an } x \in D \text{ such that } f(x) = y\}$ (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 $f: D \rightarrow C$. The *restriction* of f to the subset $B \subseteq D$ is the function $f|_B: B \rightarrow C$ given by $f|_B(b) = f(b)$ for all $b \in B$ (we also say that f is an *extension* of $f|_B$). The *image of the subset*, denoted $\text{Im}(f)$ or $f(B)$, is the range of $f|_B$. 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 $f^{-1}(A) = \{d \in D \mid f(d) \in A\}$.

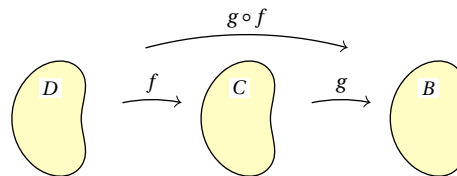
Observe that in that definition $f^{-1}(c)$ is a set, not an element.

3.10 EXERCISE. Where $f: \mathbb{R} - \{(2n + 1) \cdot \pi/2 \mid n \in \mathbb{Z}\} \rightarrow \mathbb{R}$ 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 of the sets $f^{-1}(a)$ over all $a \in A$.

COMPOSITION

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



Read $g \circ f$ aloud as “ g composed with f ” (or “ g circle f ” or “ g following 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 sometimes casual about this and don’t object as long as the domain of g includes the range of f .

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

3.14 EXERCISE. Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be $f(x) = x^2$ and let $g: \mathbb{R} \rightarrow \mathbb{R}$ be $g(x) = 3x + 1$. Find the domain, 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 specifies that for every input element there is exactly one associated output. This is asymmetric because the definition puts no such condition on output elements.

3.16 DEFINITION. A function $f: D \rightarrow C$ is *one-to-one*, or 1-1, or an *injection*, if for each value there is at most one associated argument, that is, if $f(d_0) = f(d_1)$ for $d_0, d_1 \in D$ implies that $d_0 = d_1$. The function is *onto*, or a *surjection*, if for each member of the codomain $c \in C$ there is at least one associated argument, 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 exactly one associated argument, is a *correspondence* or *bijection*.

3.17 EXERCISE. Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be $f(x) = 3x + 1$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ be $g(x) = x^2 + 1$.

- Show that f is one-to-one and onto.
- Show that g is not one-to-one and not onto.

3.18 EXERCISE. Let D and C be finite sets. Prove that if there is a correspondence $f: D \rightarrow C$ then the two have the same number of elements. *Hint:* for both you can do induction on $|C|$ or $|D|$.

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

3.19 EXERCISE. (PIGEONHOLE PRINCIPLE) Show that if you have $n > 0$ -many pigeonholes and more than n -many papers then at least one hole gets at least two papers.

3.20 EXERCISE. Prove.

- A composition of one-to-one functions is one-to-one.
- A composition of onto functions is onto. With the prior item this gives that a composition of correspondences is a correspondence.
- If $g \circ f$ is one-to-one then f is one-to-one.
- If $g \circ f$ is onto then g is onto.
- 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* $\text{id}: D \rightarrow D$ has the action $\text{id}(d) = d$ for all $d \in D$.

3.22 DEFINITION. Given $f: D \rightarrow C$, 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 *two-sided inverse*) of f , denoted f^{-1} .

3.23 EXERCISE. Show each.

- Let $g: \mathbb{R}^3 \rightarrow \mathbb{R}^2$ be the projection map $(x, y, z) \mapsto (x, y)$ and let $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ be the injection map $(x, y) \mapsto (x, y, 0)$. Then g is a left inverse of f but not a right inverse.
- The function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ given by $f(n) = n^2$ has no left inverse.
- Where $D = \{0, 1, 2, 3\}$ and $C = \{10, 11\}$, the function $f: D \rightarrow C$ 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 $f: \mathbb{Z} \rightarrow \mathbb{Z}$ is $f(a) = a + 3$ and $g: \mathbb{Z} \rightarrow \mathbb{Z}$ is $g(a) = a - 3$, show that g is inverse to f . (ii) Where $h: \mathbb{Z} \rightarrow \mathbb{Z}$ 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 $s: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is $s(x) = x^2$, find its inverse.

3.25 EXERCISE. Let $D = \{0, 1, 2\}$ and $C = \{10, 11, 12\}$. Also let $f, g: D \rightarrow C$ 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 $g: \mathbb{R} \rightarrow \mathbb{R}$ 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 $\hat{g}: \mathbb{R} \rightarrow \mathbb{R}$ 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 the definition above 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, the use of the symbol f^{-1} does not imply that the function has an inverse.

3.26 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

By definition, 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 *relation* on sets A_0, \dots, A_{n-1} is a subset of the Cartesian product, $R \subseteq A_0 \times \dots \times A_{n-1}$. If all of the sets are the same $A_0 = A_1 = \dots = A$ then we say it is a relation on A . If $n = 2$ then it is a *binary relation* on A . 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.

3.28 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{N} , (iii) $\{\langle x, y, z \rangle \in \mathbb{N}^3 \mid x^2 + y^2 = z^2\}$, (iv) $E = \{\langle x, y \rangle \in A \times \mathcal{P}(A) \mid x \in y\}$ where $A = \{0, 1, 2\}$.

3.29 EXERCISE. Verify that for any function $f: D \rightarrow C$, the set $R_f = \{\langle x, y \rangle \in D^2 \mid f(x) = f(y)\}$ is a binary relation. List six elements of R_f where f is the real function $f(x) = x^2$.

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 $\langle y, z \rangle \in R$ implies 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. For each, prove or disprove that it is reflexive, it is symmetric, and it is transitive.

- A. The "goes into" relation, $G = \{\langle d, m \rangle \in \mathbb{Z}^2 \mid d \mid m\}$.
- 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 $m \in \mathbb{Z}^+$. Show that $M = \{\langle a, b \rangle \in \mathbb{Z}^2 \mid a \equiv b \pmod{m}\}$ is an equivalence.

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

3.34 EXERCISE. There are sixteen binary relations on $A = \{0, 1\}$. Produce 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. Four of these are not reflexive. For each, give an example relation on $A = \{0, 1, 2\}$.
- B. Give examples of relations on $A = \{0, 1, 2\}$ for the other four combinations.

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 sometimes 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 $\llbracket x \rrbracket = \{y \in X \mid y \equiv x \pmod{R}\}$.

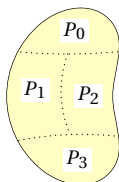
A common stumbling block is that $\llbracket x_0 \rrbracket = \llbracket x_1 \rrbracket$ does not imply that $x_0 = x_1$. An example is the relation of leaving the same remainder when divided by ten, $R = \{\langle x, y \rangle \in \mathbb{N}^2 \mid x \bmod 10 = y \bmod 10\}$. The set of numbers that leave a remainder of 1 is $\{1, 11, 21, 31, \dots\}$ and we could identify this set as the equivalence class of 1, or the equivalence class of 11, etc., $\llbracket 1 \rrbracket = \llbracket 11 \rrbracket = \llbracket 21 \rrbracket = \dots$.

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

- Two numbers $x_0, x_1 \in \mathbb{N}$ are related if they have the same parity.
- Two integers $m, n \in \mathbb{Z}$ are related if they leave the same remainder on division by 3, that is, if $m \equiv n \pmod{3}$.
- 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 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) $\llbracket x_0 \rrbracket = \llbracket x_1 \rrbracket$, and (iii) $\llbracket x_0 \rrbracket \cap \llbracket x_1 \rrbracket \neq \emptyset$.

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 $P_i \cap P_j \neq \emptyset$ 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?

- $X = \mathbb{N}$, $\mathcal{P} = \{P_0, P_1\}$, where P_0 is the set of even numbers and P_1 is the set of odd numbers.
- $X = \mathbb{Z}$, $\mathcal{P} = \{P_n \mid n \in \mathbb{Z}\}$ where $P_n = \{i \in \mathbb{Z} \mid i \equiv n \pmod{3}\}$
- $X = \mathbb{R}$, $\mathcal{P} = \{P_x \mid x \in \mathbb{R}\}$ where $P_x = \{y \in \mathbb{R} \mid x - y \in \mathbb{Z}\}$

3.42 EXERCISE. Prove.

- Where R is an equivalence on the set X , the collection of equivalence classes $\{\llbracket x \rrbracket \mid x \in X\}$ forms a partition of X . This is the partition *induced* by the relation.
- 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. Suppose that $f: D \rightarrow C$.

- Show that the relation $R_f = \{\langle d_0, d_1 \rangle \in D^2 \mid f(d_0) = f(d_1)\}$ is an equivalence on D .
- Prove that the set of inverse images $\mathcal{P} = \{f^{-1}(c) \mid c \in \text{Ran}(f)\}$ partitions the domain.
- Using that partition, consider $\hat{f}: \mathcal{P} \rightarrow \text{Ran}(f)$ 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.

- The usual less than or equal to relation, \leq , on the real numbers is a partial order.
- The relation “divides” on \mathbb{N} is a partial order.
- For any set A the relation \subseteq on $\mathcal{P}(A)$ is a partial order.

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