Proofs and Problem Solving - Cheatsheet

Based on the Fourth Edition of *A Concise Introduction to Pure Mathematics* by Marti Liebeck

Bora M. Alper
bora@boramaper.org

May 2018

caveat emptor **(/[ˌkævɛɑːt ˈɛmptɔːr]/)** "Let the buyer beware." A principle in commerce: without a warranty the buyer takes the risk.

Contents

1 Sets and Proofs

Nothing interesting.

2 Number Systems

2.1 Propositions

- **Proposition 2.1**
  Between any two rationals there is another rational.

- **Proposition 2.2**
  There is a real number α such that $\alpha^2 = 2$.

- **Proposition 2.3**
  $\sqrt{2}$ is not rational.

- **Proposition 2.4**
  Let a be a rational number, and b an irrational.

  1. Then $a + b$ is irrational.
  2. If $a \neq 0$ then ab is also irrational.

- **Proposition 2.5**
  Between any two real numbers there is an irrational.

3 Decimals

3.1 Propositions

- **Proposition 3.1**
  Let x be a real number.

  1. If $x \neq 1$, then

  $$x + x^2 + x^3 + \ldots + x^n = \frac{x(1 - x^n)}{1 - x}$$

  2. If $-1 < x < 1$, then the sum to infinity is

  $$x + x^2 + x^3 + \ldots = \frac{x}{1 - x}$$

- **Proposition 3.2**
  Every real number x has a decimal expression

  $$x = a_0.a_1a_2a_3\ldots$$

- **Proposition 3.3**
  Suppose that $a_0.a_1a_2a_3\ldots$ and $b_0.b_1b_2b_3\ldots$ are two different decimal expressions for the same real number. Then one of these expressions ends in $9999\ldots$ and the other ends in $0000\ldots$

- **Proposition 3.4**
  The decimal expression for any rational number is periodic.

- **Proposition 3.5**
  Every periodic decimal is rational.

3.2 Hints

- Periodicity is almost always when divided by 99.

4 n^{th} Roots and Rational Powers

4.1 Propositions

- **Proposition 4.1**
  Let n be a positive integer. If x is a positive real number, then there is exactly one positive real number y such that $y^n = x$.

  - Positive integer powers of every positive integer is (a) unique (positive integer).

- **Proposition 4.2**
  Let x, y be positive real numbers and $p, q \in \mathbb{Q}$. Then

  1. $x^p x^q = x^{p+q}$
  2. $(x^p)^q = x^{pq}$
  3. $(xy)^p = x^p y^p$

5 Inequalities

5.1 Rules

- **Rule 5.1**

  1. If $x \in \mathbb{R}$, then either $x > 0$ or $x < 0$ or $x = 0$ (and just one of these is true).
  2. If $x > y$ then $-x < -y$.
  3. If $x > y$ and $c \in \mathbb{R}$, then $x + c > y + c$.
  4. If $x > 0$ and $y > 0$, then $xy > 0$.
  5. If $x > y$ and $y > z$ then $x > z$.

6 Complex Numbers

6.1 Notations

- **Notation 6.1 (The $e^{i\theta}$ Notation)**

$$re^{i\theta} = r(\cos\theta + i\sin\theta)$$

6.2 Definitions

- **Definition 6.X (Roots of Unity)**
  Let n be a positive integer, then the complex numbers that satisfy the equation

$$z^n = 1$$

  are called the n^{th} roots of unity.

6.3 Theorems

- **Theorem 6.1 (De Moivre's Theorem)**
  Let z_1, z_2 be complex numbers with polar forms

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1), \quad z_2 = r_2(\cos\theta_2 + i\ \sin\theta_2)$$

  Then the product

$$z_1 z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + i\ \sin(\theta_1 + \theta_2))$$

  In other words, $z_1 z_2$ has modulus $r_1 r_2$ and argument $\theta_1 + \theta_2$.

  De Moivre's Theorem says that multiplying a complex number z by $\text{cos}\theta + i\text{sin}\theta$ rotates z counter-clockwise through the angle θ.

6.4 Propositions

- **Proposition 6.1**
  Let $z = r(\cos\theta + i\sin\theta)$, and let n be a positive integer. Then

  1. $z^n = r^n(\cos n\theta + i\sin n\theta)$, and
  2. $z^{-n} = r^{-n}(\cos n\theta - i\sin n\theta)$.

- **Proposition 6.2**

  1. If $z = re^{i\theta}$ then $\overline{z} = re^{-i\theta}$.

2. Let $z = re^{i\theta}$, $w = se^{i\phi}$ in polar form. Then $z = w$ if and only if both $r = s$ and $\theta - \phi = 2k\pi$ with $k \in \mathbb{Z}$.

- **Proposition 6.3**
  Let n be a positive integer and define $w = e^{\frac{2\pi i}{n}}$. Then the n^{th} roots of unity are n complex numbers

$$1, w, w^2, \ldots, w^{n-1}$$

7 Polynomial Equations

7.1 Theorems

- **Theorem 7.1 (Fundamental Theorem of Algebra)**
  Every polynomial equation of degree at least 1 has a root in $\mathbb{C}$.

- **Theorem 7.2**
  Every polynomial of degree n factorises as a product of linear polynomials and has exactly n roots in $\mathbb{C}$ (counting repeats).

- **Theorem 7.3**
  Every real polynomial factorises as a product of real linear and real quadratic polynomials (which contains the complex conjugate pair roots).

7.2 Propositions

- **Proposition 7.1**
  Let the roots of the equation

  $$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

  be $\alpha_1, \alpha_2, \ldots, \alpha_n$. If s_1 denotes the sum of the roots, s_2 denotes the sum of all products of **pairs** of roots, s_3 denotes the sum of all products of **triples** of roots, and so on, then

  $$\begin{aligned} s_1 = \alpha_1 + \ldots + \alpha_n &= -a_{n-1}, \\ s_2 &= +a_{n-2}, \\ s_3 &= -a_{n-3}, \\ &\vdots \\ s_n = \alpha_1\alpha_2 \ldots \alpha_n &= (-1)^n a_0 \end{aligned}$$

8 Induction

8.1 Propositions

- **Proposition 8.1**
  Every positive integer greater than 1 is equal to a product of prime numbers.

- **Proposition 8.2**
  Let n be a positive integer. Then for any real numbers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$,

$$a_1 b_1 + \ldots + a_n b_n \leq \sqrt{a_1^2 + \ldots + a_n^2}\sqrt{b_1^2 + \ldots + b_n^2}$$

9 Euler's Formula and Platonic Solids

9.1 Definition

- **Definition 9.X**
  A **polyhedron** is a solid whose surface consists of a number of faces, all of which are polygons, such that any side of a face lies on exactly one other face. The corners of the faces are called the **vertices** of the polyhedron, and their sides are the **edges**.

- **Definition 9.1**
  A **plane graph** is a figure in the plane consisting of a collection of points (vertices), and some edges joining various pairs of these points, with **no two edges crossing each other**. A plane graph is **connected** if we can get from any vertex of the graph to any other vertex by going along a path of edges in the graph.

- **Definition 9.X**
  A polygon is said to be **regular** if all its sides are of equal length and all its internal angles are equal too.

- **Definition 9.X**
  A polyhedron is **regular** if its faces are regular polygons, all with the same number of sides, and also each vertex belongs to the same number of edges.

  Platonic (Regular) Solids

	V	E	F	n	r
tetrahedron	4	6	4	3	3
cube	8	12	6	4	3
octahedron	6	12	8	3	4
icosahedron	12	30	20	3	5
dodecahedron	20	30	12	5	3

  V Vertices

  E Edges

  F Faces

  n Number of sides on a face

  r Number of edges each vertex belongs to

9.2 Theorems

- **Theorem 9.1**
  For a corner polyhedron with V vertices, E edges and F faces, we have
  $$V - E + F = 2$$
- **Theorem 9.2**
  If a connected plane graph has v vertices, e edges and f faces, then
  $$v - e + f = 1$$
- **Theorem 9.3**
  The only regular convex polyhedra are the five Platonic solids.

10 The Integers

10.1 Definitions

- **Definition 10.1**
  Let $a, b \in \mathbb{Z}$. We say a **divides** b (or a is a factor of b) if $b = ac$ for some integer c. When a divides b, we write $a|b$.

- **Definition 10.2**
  Let $a, b \in \mathbb{Z}$. A common factor of a and b is an integer that divides both a and b. The **highest common factor** (*i.e.* **greatest common divisor**) of a and b, written $\text{hcf}(a, b)$ or $\text{gcd}(a, b)$, is the largest positive integer that divides both a and b.

  - See page 88 for Euclid's Algorithm.

- **Definition 10.3**
  If $a, b \in \mathbb{Z}$ and $\text{hcf}(a, b) = 1$, we say that a and b are **coprime to each other**.

10.2 Propositions

- **Proposition 10.1**
  Let a be a a positive integer. Then for any $b \in \mathbb{Z}$, there are integers q, r such that

  $$b = qa + r \quad \text{and} \quad 0 \leq r < a$$

  The integer q is called the quotient, and r is the remainder.

- **Proposition 10.2**
  Let $a, b, d \in \mathbb{Z}$, and supposed that $d|a$ and $d|b$. Then $d|(ma + nb)$ for any $m, n \in \mathbb{Z}$.

- **Proposition 10.3**
  If $a, b \in \mathbb{Z}$ and $d = \text{hcf}(a, b)$, then there are integers s and t such that

  $$d = sa + tb$$

- **Proposition 10.4**
  If $a, b \in \mathbb{Z}$, then any common factor of a and b also divides $\text{hcf}(a, b)$.

- **Proposition 10.5**
  Let $a, b \in \mathbb{Z}$

1. Suppose c is a integer such that a and c are coprime to each other, and $c|ab$. Then $c|b$.
2. Suppose p is a prime number and $p|ab$. Then either $p|a$ or $p|b$ or both.

- **Proposition 10.6**
  Let $a_1, a_2, \dots, a_n \in \mathbb{Z}$, and let p be a prime number. If $p|a_1a_2\dots a_n$, then $p|a_i$ for some i.

11 Prime Factorization

11.1 Theorems

- **Theorem 11.1 (Fundamental Theorem of Arithmetic)**
  Let n be an integer with $n \geq 2$.

  1. Then n is equal to a product of prime numbers: we have

  $$n = p_1 \ldots p_k$$

  where $p_1, \ldots, p_k$ are primes and $p_1 \leq p_2 \leq \ldots \leq p_k$.

  2. This prime factorisation of n is unique: in other words, if

  $$n = p_1 \ldots p_k = q_1 \ldots q_l$$

  where p_is and q_is are all prime, $p_1 \leq p_2 \leq \ldots \leq p_k$ and $q_1 \leq q_2 \leq \ldots \leq q_l$, then

  $$k = l \quad \text{and} \quad p_i = q_i, \ \forall i = i, \ldots, k$$

11.2 Propositions

- **Proposition 11.1**
  Let $n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, where p_is are prime, $p_1 < p_2 < \ldots < p_m$ and a_is are positive integers. If $m|n$, then

  $$m = p_1^{b_1} p_2^{b_2} \ldots p_m^{b_m} \quad \text{with} \quad 0 \leq b_i \leq a_i, \ \forall i \in [i, m]$$

  For example, the only divisors of 2^1003^2 are the numbers $2^a 3^b$, where $0 \leq a \leq 100$, $0 \leq b \leq 2$.

- **Proposition 11.2**
  Let $a, b \geq 2$ be integers with prime factorisations

  $$a = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}, \ b = p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m}$$

  where the p_i are distinct primes and all $r_i, s_i \geq 0$ (we allow some of the r_i and s_i to be 0). Then

  1. $\text{hcf}(a, b) = p_1^{\min(r_1, s_1)} \ldots p_m^{\min(r_m, s_m)}$
  2. $\text{lcm}(a, b) = p_1^{\max(r_1, s_1)} \ldots p_m^{\max(r_m, s_m)}$
  3. $\text{lcm}(a, b) = ab / \text{hcf}(a, b)$

- **Proposition 11.3**
  Let n be a positive integer. Then $\sqrt{n}$ is rational if and only if n is a perfect square (*i.e.* $n = m^2$ for some integer m).

- **Proposition 11.4**
  Let a and b be positive integers that are coprime to each other.

  1. If ab is a square, then both a and b are also squares.
  2. More generally, if ab is an n^{th} power (for some positive integer n), then both (a and b are also n^{th} powers.

12 More on Prime Numbers

12.1 Theorems

- **Theorem 12.1**
  There are infinitely many prime numbers.

- **Theorem 12.2**
  For a positive integer n, let $\pi(n)$ be the number of primes up to n. Then the ratio of $\pi(n)$ and $\frac{n}{log_e n}$ tends to 1 as n tends to infinity.

13 Congruence of Integers

13.1 Definitions

- **Definition 13.1**
  Let m be a positive integer. For $a, b \in \mathbb{Z}$, if m divides $b - a$ we write $a \equiv b \mod m$ and say a is **congruent** to b modulo m.

- **Definition 13.X (The System $\mathbb{Z}_m$)**
  $\mathbb{Z}_m$ denotes "the non-negative integers modulo m". For example

$$\begin{aligned} \mathbb{Z}_4 &= 0, 1, 2, 3 \\ \mathbb{Z}_8 &= 0, 1, 2, 3, 4, 5, 6, 7 \\ &\vdots \end{aligned}$$

13.2 Propositions

- **Proposition 13.1**
  Every integer is congruent to exactly one of the numbers $0, 1, 2, \ldots, m-1$ modulo m.

- **Proposition 13.2**
  Let m be a positive integer. The following are true, $\forall a, b, c \in \mathbb{Z}$:

  1. $a \equiv a \mod m$,
  2. if $a \equiv b \mod m$ then $b \equiv a \mod m$,
  3. if $a \equiv b \mod m$ **and** $b \equiv c \mod m$, then $a \equiv c \mod m$.

- **Proposition 13.3**
  Suppose $a \equiv b \mod m$ and $c \equiv d \mod m$. Then

$$a + c \equiv b + d \mod m \qquad \text{and} \qquad ac \equiv bd \mod m$$

- **Proposition 13.4**
  If $a \equiv b \mod m$, and n is a positive integer, then

$$a^n \equiv b^n \mod m$$

- **Proposition 13.5.1**
  Let a and m be coprime integers. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \mod m$, then $x \equiv y \mod m$.

- **Proposition 13.5.2**
  Let p be a prime, and let a be an integer that is not divisible by p. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \mod p$, then $x \equiv y \mod p$.

- **Proposition 13.6**
  The congruence equation

  $$ax \equiv b \mod m$$

  has a solution $x \in \mathbb{Z}$ **if and only if** $\mathrm{hcf}(a, m)$ divides b.

14 More on Congruence

14.1 Theorems

- **Theorem 14.1 (Fermat's Little Theorem)**
  Let p be a prime number, and let a be an integer that is not divisible by p. Then
  $$a^{p-1} \equiv 1 \mod p$$
  - For example for $p = 17$
  $$\begin{aligned} 2^{16} &\equiv 1 \mod 17 \\ 93^{16} &\equiv 1 \mod 17 \\ 72307892^{16} &\equiv 1 \mod 17 \end{aligned}$$

14.2 Propositions

- **Proposition 14.1**
  Let p and q be distinct prime numbers, and let a be an integer that is not divisible by p or q. Then
  $$a^{(p-1)(q-1)} \equiv 1 \mod pq$$
- **Proposition 14.2**
  Let p be a prime, and let k be a positive integer coprime to $p-1$. Then
  1. $\exists s \in \mathbb{Z}^+$ such that $sk \equiv 1 \mod (p-1)$, and
  2. for $\forall b \in \mathbb{Z}$ not divisible by p, the congruence equation
  $$x^k \equiv b \mod p$$
  has a unique solution for x modulo p. This solution is $x \equiv b^s \mod p$, where s is as in (1.).
- **Proposition 14.3**
  Let p, q be distinct primes, and let k be a positive integer coprime to $(p-1)(q-1)$. Then
  - $\exists s \in \mathbb{Z}^+$ such that $sk \equiv 1 \mod (p-1)(q-1)$, and
  - $\forall b \in \mathbb{Z}$ not divisible by p or q, the congruence equation
  $$x^k \equiv b \mod pq$$
  has a unique solution for x modulo pq. This solution is $x \equiv b^s \mod pq$, where s is as in (1.).

- **Proposition 14.4**
  Let p be a prime. If a is an integer such that $a^2 \equiv 1 \mod p$, then $a \equiv \pm 1 \mod p$.

15 Secret Codes

Nothing (but *very* interesting)!

16 Counting and Choosing

16.1 Definitions

- **Definition 16.1 (Binomial Coefficients)**
  Let n be a positive integer and r an integer such that $0 \leq r \leq n$. Define

  $$\binom{n}{r}$$

  (called "n choose r") to be the number of r-element subsets of $\{1, 2, \ldots, n\}$.

- **Definition 16.2 (Ordered Partitions [Multinomial Coefficients])**
  Let n be a positive integer, and let $S = \{1, 2, \ldots, n\}$. A **partition** of S is a collection of subsets $S_1, \ldots, S_k$ such that each element of S lies in exactly one of these subsets. The partition is **ordered** if we take account of the order in which the subsets are written.

  The point about the order is that, for instance, the ordered partition

  $$\{1, 2, 3, 4\} \quad \{5, 6\} \quad \{7, 8\}$$

  is different from the ordered partition

  $$\{1, 2, 3, 4\} \quad \{7, 8\} \quad \{5, 6\}$$

  even though the subsets involved are the same in both cases.

  If $r_1, r_2, \ldots, r_k$ are non-negative integers such that $n = r_1 + r_2 + \ldots + r_k$, we denote the total number of ordered partitions of $S = \{1, 2, \ldots, n\}$ into subsets $S_1, S_2, \ldots, S_k$ of sizes $r_1, r_2, \ldots, r_k$ by the symbol

  $$\binom{n}{r_1, r_2, \ldots, r_k}$$

16.2 Theorems

- **Theorem 16.1 (Multiplication Principle)**
  Let P be a process which consists of n stages, and suppose that for each r, the r^{th} stage can be carried out in a_r ways. Then P can be carried out in $a_1 a_2 \ldots a_n$ ways.

- **Theorem 16.2 (Binomial Theorem)**
  Let n be a positive integer, and let a, b be real numbers. Then

$$\begin{aligned}(a+b)^n &= \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r \\ &= a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \ldots + \binom{n}{n-1} a b^{n-1} + b^n\end{aligned}$$

- **Theorem 16.3 (Multinomial Theorem)**
  Let n be a positive integer, and let $x_1, \ldots, x_k$ be a real numbers. Then the expansion of $(x_1 + x_2 + \ldots + x_k)^n$ is the sum of all terms of the form

$$\binom{n}{r_1, r_2, \ldots, r_k} x_1^{r_1} x_2^{r_2} \ldots x_k^{r_k}$$

  where $r_1, r_2, \ldots, r_k$ are non-negative integers such that $r_1 + r_2 + \ldots + r_k = n$

16.3 Propositions

- **Proposition 16.1**
  Let S be a set consisting of n elements. Then the number of different arrangements of the elements of S **in order** is $n!$

  Recall that $n! = n \cdot (n-1) \cdot (n-2) \ldots 2 \cdot 1$

- **Proposition 16.2**

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

- **Proposition 16.3**
  For any positive integer n,

$$(x+1)^n = \sum_{r=0}^{n} \binom{n}{r} x^r$$

  Putting $x = \pm 1$ in this, we get the interesting equalities

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n, \qquad \sum_{r=0}^{n} (-1)^n \binom{n}{r} = 0$$

  The second of these equalities gives the following:

$$\sum_{r=1}^{n} (-1)^{r-1} \binom{n}{r} = \binom{n}{0} = 1$$

- **Proposition 16.4**
  Let S be a set of n elements.

  1. The number of ordered selections of r elements of S, allowing **repetitions**, is equal to n^r.
  2. The number of ordered selections of r **distinct** elements of S is equal to $n(n-1)\dots(n-r+1)$

- **Proposition 16.5**

$$\binom{n}{r_1, r_2, \dots, r_k} = \frac{n!}{r_1! r_2! \dots r_k!}$$

16.4 Examples

- **Example 16.9**
  Find the coefficient of x^3 in the expansion of $(1 - \frac{1}{x^3} + 2x^2)^5$.

  A **typical** term in this expansion is

$$\binom{5}{a, b, c} \cdot 1^a \cdot \left(\frac{-1}{x^3}\right)^b \cdot \left(2x^2\right)^c$$

where $a+b+c=5$ (and $a, b, c \geq 0$). To make this a term in x^3, we need

$$-3b + 2c = 3 \qquad \text{and} \qquad a+b+c=5$$

From the first equation, 3 divides c, so $c=0$ or 3. If $c=0$ then $b=-1$, which is impossible. Hence $c=3$, and it follows that $a=1$, $b=1$. Thus there is just one term in x^3, namely

$$\binom{5}{1,1,3} \cdot 1 \cdot \left(\frac{-1}{x^3}\right) \cdot \left(2x^2\right)^3$$

In other words, the coefficient is $\binom{5}{1,1,3} = -160$.

17 More on Sets

17.1 Definitions

- **Definition 17.1 (Euler's ϕ-Function)**
  For a positive integer n, define $\phi(n)$ to be the number of integers x such that $1 \leq x \leq x$ and $\text{hcf}(x, n) = 1$. The function ϕ is known as the **Euler's ϕ-function**.

17.2 Theorems

- **Theorem 17.1 (Inclusion-Exclusion Principle)**
  Let n be a positive integer, and let $A_1, A_2, \ldots, A_n$ be finite sets. Then
  $$|A_1 \cup A_2 \cup \ldots \cup A_n| = c_1 - c_2 + c_3 - \ldots + (-1)^n c_n$$
  where for $1 \leq i \leq n$, the number c_i is the sum of the **sizes of the intersections** of the sets taken i at a time.

  For instance for $n = 3$,
  $$\begin{aligned} c_1 &= |A_1| + |A_2| + |A_3| \\ c_2 &= |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| \\ c_3 &= |A_1 \cap A_2 \cap A_3| \end{aligned}$$

17.3 Propositions

- **Proposition 17.2**
  If A and B are finite sets, then
  $$|A \cup B| = |A| + |B| - |A \cap B|$$

- **Proposition 17.3**
  Let $n \geq 2$ be an integer with prime factorization $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ (where the primes p_i are distinct and all $a_1 \geq 1$). Then
  $$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$
  For example for $n = 420 = 2^2 \cdot 3 \cdot 5 \cdot 7$,
  $$\phi(420) = 420 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 96$$

- **Proposition 17.4**
  Let S be a finite set consisting of n elements. Then the total number of subsets of S is equal to 2^n.

18 Equivalence Relations

18.1 Definitions

- **Definition 18.1 (Reflexivity, Symmetry, Transitivity)**
  Let S be a set, and let $\sim$ be a **relation** on S. Then $\sim$ is an **equivalence relation** if the following 3 properties hold for all $a, b, c \in S$:

  1. $a \sim a$ (reflexive)
  2. if $a \sim b$ then $b \sim a$ (symmetric)
  3. if $a \sim b$ and $b \sim c$ then $a \sim c$ (transitive)

- **Definition 18.2 (Equivalence Classes)**
  Let S be a set and $\sim$ an equivalence relation on S. For $a \in S$, define

  $$\mathrm{cl}(a) = \{s \mid s \in S, s \sim a\}$$

  Thus $\mathrm{cl}(a)$ is the set of things that are related to a. The subset $\mathrm{cl}(a)$ is called **an equivalence class** of $\sim$. The equivalence class**es** of $\sim$ are the subsets $\mathrm{cl}(a)$ as a ranges over the elements of S.

  For instance, let m be a positive integer, and let $\sim$ be the equivalence relation on $\mathbb{Z}$ defined as:

  $$a \sim b \quad \iff \quad a \equiv b \mod m$$

  The equivalence classes of this relation is:

  $$\begin{aligned} \mathrm{cl}(0) &= \{s \in \mathbb{Z} \mid s \equiv 0 \mod m\} \\ \mathrm{cl}(0) &= \{s \in \mathbb{Z} \mid s \equiv 1 \mod m\} \\ &\vdots \\ \mathrm{cl}(m-1) &= \{s \in \mathbb{Z} \mid s \equiv m-1 \mod m\} \end{aligned}$$

  These are **all** the equivalence classes.

18.2 Propositions

- **Proposition 18.1**
  Let S be a set and let $\sim$ be an equivalence relation on S. Then the equivalence classes of $\sim$ form a partition of S.

  There is a very tight correspondence between the equivalence relations on a set S and the partitions of S: every equivalence relation gives a unique partition of S, and every partition gives a unique equivalence relation.

19 Functions

19.1 Definitions

- **Definition 19.1**
  Let S and T be sets. A **function** from S to T is a rule that assigns to each $s \in S$ a single element of T, denoted by $\mathrm{f}(s)$. We write

  $$\mathrm{f} : S \to T$$

  to mean that f is a function from S to T. If $\mathrm{f}(s) = t$, we often say f sends $s \to t$.

  If $\mathrm{f} : S \to T$ is a function, the **image** of f is the set of all elements of T that are equal to $\mathrm{f}(s)$ for some $s \in S$. We write $\mathrm{f}(S)$ for the image of f. Thus

  $$\mathrm{f}(S) = \{\mathrm{f}(s) \mid s \in S\}$$

- **Definition 19.2**
  Let $\mathrm{f} : S \to T$ be a function.

  1. We say f is **onto** (or **surjective**) if the image $\mathrm{f}(S) = T$; *i.e.* if for every $t \in T$ there exists $s \in S$ such that $\mathrm{f}(s) = t$. [range is completely mapped]
  2. We say f is **one-to-one** (or **injective**) if for for all distinct $s_1, s_2 \in S$, $\mathrm{f}(s_1) \neq f(s_2)$; *i.e.* f sends different elements of S to different elements of T. Yet another way of putting this is to say:

     $$\forall s_1, s_2 \in S, \quad \mathrm{f}(s_1) = \mathrm{f}(s_2) \implies s_1 = s_2$$

  3. We say f is a **bijective** function if f is both onto and 1-1.

- **Definition 19.3 (The Pigeonhole Principle)**
  Part (2.) of Proposition 19.1 implies that if $|S| > |T|$, then there is no 1-1 function from S to T. This can be phrased in the following way:

  If we put $n+1$ or more pigeons into n pigeonholes, then there must be a pigeonhole containing more than one pigeon.

  Always **try defining what "pigeons" and "pigeonholes" are**, while trying to apply the technique for a given question.

- **Definition 19.3 (Inverse Functions)**
  Let $\mathrm{f} : S \to T$ be a **bijection**. We denote the inverse function by $\mathrm{f}^{-1} : T \to S$ such that

  $$\forall s \in S, t \in T, \quad \mathrm{f}^{-1}(t) = s \iff \mathrm{f}(s) = t$$

19.2 Propositions

- **Proposition 19.1**
  Let f : $S \to T$ be a function, where S and T are finite sets.

  1. If f is **onto**, then $|S| \geq |T|$.
  2. If f is **one-to-one**, then $|S| \leq |T|$.
  3. If f is **bijective**, then $|S| = |T|$.

- **Proposition 19.2**
  Let S, T, U be sets, and let f : $S \to T$ and g : $T \to U$ be functions. Then

  1. if f and g are both 1-1, so is $g \circ f$,
  2. if f and g are both onto, so is $g \circ f$,
  3. if f and g are both bijective, so is $g \circ f$.

- **Proposition 19.3**
  Let S, T be finite sets, then the **number of functions** $S \to T$ is equal to
  $$|T|^{|S|}$$

- **Proposition 19.X**
  Let S, T be finite sets, then the **number of injective functions** $S \to T$ is equal to
  $$\frac{|T|!}{(|T| - |S|)!}$$

20 Permutations

Even and Odd Permutations (*i.e.* signs) are skipped.

20.1 Notations

- **Notation 20.1 (The Cycle Notation)**
  Consider the following permutation in S_8:

  $$\mathrm{f} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 3 & 2 & 7 & 1 & 8 \end{pmatrix}$$

  This sends $1 \to 4$, $4 \to 3$, $3 \to 6$, $6 \to 7$, and 7 back to 1; we say that symbols 1, 4, 3, 6, 7 form a **cycle** of f (of length 5). Similarly, 2 and 5 form a cycle of length 2 and 8 forms a cycle of length 1. We write

  $$\mathrm{f} = (14367)(25)(8)$$

  This notation indicates that each number 1, 4, 3, 6, 7 in the first cycle goes to the next one, except for the last, which goes back to the first; and likewise for the second and third cycles.

  Notice that the cycles have no symbols in common; they are called **disjoint** cycles.

20.2 Definitions

- **Definition 20.X (Permutations)**
  Let S be a set. By **permutation** of S, we mean a bijection $S \to S$ - that is, a function $S \to S$ that is both onto and 1-1.

  For instance, let $S = \{1, 2, 3, 4, 5\}$ and let $\mathrm{f} : S \to S$ and $\mathrm{g} : \mathbb{R} \to \mathbb{R}$ be defined as follows:

  $$\begin{aligned} \mathrm{f} \ &: \ 1 \to 2, \ 2 \to 4, \ 3 \to 3, \ 4 \to 5, \ 5 \to 1 \\ \mathrm{g}(x) &= 8 - 2x \end{aligned}$$

  Then f is a permutation of S, and g is a permutation of $\mathbb{R}$.

- **Definition 20.X (Composition of Permutations)**
  If f and g are both permutations of a set S, the composition $\mathrm{f} \circ \mathrm{g}$ is also a permutation of S.

- **Definition 20.X (Cycle-Shape)**
  If $g \in S_n$ is a permutation given in cycle notation, the cycle-shape of g is the sequence of numbers we get by writing down the lengths of the disjoint cycles of g in decreasing order.

  For example, the cycle-shape of the permutation (163)(24)(58)(7)(9) is S_9 is $(3, 2, 2, 1, 1)$; which could be written more succinctly as $(3, 2^2, 1^2)$.

- **Definition 20.X (Order of a Permutation)**
  We define order of a permutation $g \in S_n$ to be the smallest positive integer r such that $g^r = i$. In other words, the orer of g is the smallest number of times we have to do g to send everything back to where it came from.

20.3 Propositions

- **Proposition 20.1**
  The number of permutations in S_n (a set with n elements) is $n!$

- **Proposition 20.2**
  The following properties are true for the set S_n of all permutations of $\{1, 2, \ldots, n\}$:

  1. If f and g are in S_n, so is $f \circ g$
  2. For any $f, g, h \in S_n$
  $$f \circ (g \circ h) \; = \; (f \circ g) \circ h$$
  3. The identity permutation $i \in S_n$ satisfies
  $$f \circ i \; = \; i \circ f \; = \; f$$
  for any $f \in S_n$
  4. Every permutation $f \in S_n$ has an inverse $f^{-1} \in S_n$ such that
  $$f \circ f^{-1} \; = \; f^{-1} \circ f \; = \; i$$

- **Proposition 20.3**
  Every permutation of S_n can be expressed as a product of disjoint cycles.

- **Proposition 20.4**
  The order of a permutation in cycle notation is equal to the least common multiple of the lengths of the cycles.

21 Infinity

21.1 Definitions

- **Definition 21.1**
  Two sets A and B are said to be **equivalent** to each other if there is a bijection from A to B. We write $A \sim B$ if A and B are equivalent to each other.

- **Definition 21.2 (Countable Sets)**
  A set A is said to be countable if A is equivalent to $\mathbb{N}$. In other words, A is countable if it is an infinite set, all of whose elements can be listed as $A = \{a_1, a_2, a_3, \ldots, a_n, \ldots\}$.

- **Definition 21.3 (Cardinality)**
  Let A and B be sets. If A and B are equivalent to each other (*i.e.* there is a bijection $A \to B$), we say that A and B have the same cardinality, and we write $|A| = |B|$.

  If there is a 1-1 function $A \to B$, we write $|A| \leq |B|$.

  And if there is a 1-1 function $A \to B$, but no bijection $A \to B$, we write $|A| < |B|$, and say that A has smaller cardinality than B. (Thus, $|A| < |B|$ is the same as saying that $|A| \leq |B|$ and $|A| \neq |B|$.)

- **Definition 21.4 (A Hierarchy of Infinities)**
  If S is a set, let $\mathrm{P}(S)$ be the set consisting of all the subsets of S.

21.2 Theorems

- **Theorem 21.1**
  The set $\mathbb{R}$ of all real numbers is uncountable.

21.3 Propositions

- **Proposition 21.1**
  The relation $\sim$ defined in Definition (1) is an equivalence relation (*i.e.* satisfies the criterion of reflexivity, symmetry, and transitivity).

- **Proposition 21.2**
  Every infinite subset of $\mathbb{N}$ is countable.

- **Proposition 21.3**
  The set of rationals $\mathbb{Q}$ is countable.

- **Proposition 21.4**
  Let S be an infinite set. If there is a 1-1 function $\mathrm{f} : S \to \mathbb{N}$, then S is countable.

  Because consequently, there is a bijection $\mathrm{g} : \mathbb{N} \to \mathrm{f}(S)$

- **Proposition 21.5**
  Let S be a set. Then there is **no bijection** $S \to \mathrm{P}(S)$. Consequently, $|S| < |\mathrm{P}(S)|$.

  Using the proposition, we obtain a hierarchy of infinities, starting at $|\mathbb{N}|$:
  $$|\mathbb{N}| < |\mathrm{P}(\mathbb{N})| < |\mathrm{P}(\mathrm{P}(\mathbb{N}))| < |\mathrm{P}(\mathrm{P}(\mathrm{P}(\mathbb{N})))| < \ldots$$

  Thus there are indeed many types of "infinity."

22 Introduction to Analysis: Bounds

Skipped; pray to your favourite deity.

A Appendix

A.1 Methods of Proofs

- **Direct Proof**
- **Proof by Induction**
  Applicable only when working with operations on countable sets (where the notion of *next item* makes any sense).

  1. Prove the base case $\mathrm{P}(b)$
  2. Prove that if $\mathrm{P}(x)$ is true, then $\mathrm{P}(x+1)$

  Hence $\mathrm{P}(x)$ is true $\forall x \in [b, \infty)$.

- **Proof by Contrapositive**
  To prove $\mathrm{P} \implies \mathrm{Q}$:

  1. Assume $\neg\mathrm{Q}$
  2. Prove $\neg\mathrm{P}$

- **Proof by Contradiction**
  To prove $\mathrm{P} \implies \mathrm{Q}$:

  1. Assume **both** P and $\neg\mathrm{Q}$
  2. Deduce some (other) contradiction such as $\mathrm{R} \wedge \neg\mathrm{R}$