Chapter 11: Properties of Finite Sets

The Pigeonhole Principle:

Last time (i.e. in the notes on chapter 10) we proved "Proposition A":

Proposition 11.1.4: Suppose $f: X \to \mathbb{N}_n$ is an injection. Then X is finite and $|X| \leq n$.

The following is an immediate corollary.

Corollary 11.1.5: Suppose $X \subseteq Y$, where Y is a finite set. Then X is also finite and $|X| \leq |Y|$.

Proposition 11.1.4 also implies:

Corollary 11.1.1: Let X and Y be finite sets. If there exists an injection $f: X \to Y$ then $|X| \leq |Y|$

↑ We don't really need to assume that X is finite here (see Corollary A from last time), but we state the result this way because the next result we want to state is just the contrapositive of this.

Taking the contrapositive of Corollary 11.1.1 we get:

Theorem 11.1.2 (The pigeonhole principle):

Let X and Y be finite sets. If $|X| > |Y|$ then any map $f: X \to Y$ fails to be injective.

Alternative Statements of the Pigeonhole Principle:

- Let X and Y be finite sets with $|X| > |Y|$. If $f: X \to Y$ then $\exists\, x_1, x_2 \in X$ with $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.
- Let $m, n \in \mathbb{N}$, $m > n$. If m marbles are placed in n drawers, then at least one drawer contains more than one marble.
- "If $n+1$ pigeons are placed in n pigeonholes, then (exactly) one pigeonhole contains two pigeons."

Example Applications:

This is a very useful theorem/principle

- In a group of 13 or more people there must be two people with birthdays in the same month.
- There are two people in San Diego with the

same number of hairs on their head.

- This is because people have less than 1 million hairs on their head and San Diego has more than 1 million people.

- **Proposition:** Let A be a subset of $\underbrace{\{1,\dots,2n\}}_{\mathbb{N}_{2n}}$ with $|A| = n+1$. Then A contains a pair of consecutive integers a and $a+1$.

Proof:

Let $A_k = \{2k-1, 2k\}$ for each $k \in \{1,\dots,n\}$.
(That is, $A_1 = \{1,2\}$, $A_2 = \{3,4\}$, $\dots$, $A_n = \{2n-1, 2n\}$.)
Let $B = \{A_1, \dots, A_n\}$ and let $f: A \to B$ be defined by $a \mapsto f(a)$ where $f(a)$ is the unique set $A_k \in B$ s.t. $a \in A_k$. Then, by the pigeonhole principle, f is not injective. So $\exists\ x, y \in A$ with $x \neq y$ and $f(x) = f(y)$, i.e. with $x \neq y$ and with x and y both being elements of the same set $A_k = \{2k-1, 2k\}$. So $\{x, y\} = \{2k-1, 2k\}$ is a subset of A. □

The first proof illustrates the connection with a function f.

A more natural way to write the proof:

Let $A_k = \{2k-1, 2k\}$ for each $k \in \{1,\dots,n\}$.
By the pigeonhole principle A must contain one of the sets A_k (if A only contained one of

the elements from each of the sets A_k, then A would only have n elements). It follows that A contains two consecutive integers. □

The following is an immediate consequence of "Proposition B":

Theorem 11.1.6: Let X and Y be finite sets. If $|X| < |Y|$ then any map $f: X \to Y$ fails to be surjective.

One can also easily prove (homework):

Theorem 11.1.7: Let X and Y be non-empty finite sets with $|X| = |Y|$. Then $f: X \to Y$ is an injection if and only if it is a surjection.

(Thus to prove bijectivity one only needs to check injectivity or surjectivity, presuming of course that X and Y are non-empty, finite, and $|X| = |Y|$.)

The Greatest Common Divisor

Def^n: Let $A \subseteq \mathbb{R}$ be nonempty. Then $b \in A$ a minimum of A if

$$\forall a \in A, \quad b \leq a.$$

If A has a minimum, then it is unique.

Notation: $b = \min A$.

Def^n (cont.): Similarly, $c \in A$ is a **maximum** of A if

$$\forall a \in A, \quad a \leq c.$$

Notation: $c = \max A$.

If A has a maximum, then it is unique.

Examples:

- If $A = \{-1, 2, 5\}$ then $\min A = -1$, $\max A = 5$.

Let $a, b \in \mathbb{R}$ with $a < b$.

- The open interval $(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$ has no maximum and no minimum.
- The closed interval $[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ has $\max [a,b] = b$ and $\min [a,b] = a$.
- The interval $[a,b) = \{x \in \mathbb{R} \mid a \leq x < b\}$ has $\min [a,b) = a$ and has no maximum.
- **Well-ordering principle:** Any non-empty set of natural numbers has a minimum element.
  (Hence any non-empty set of natural numbers can be "listed" from smallest to "largest" — of course there may not be a "largest" element and so the "list" may go on forever.)

The well-ordering principle is equivalent to the principle of mathematical induction.

Proposition 11.2.3: Let $A \subseteq \mathbb{R}$ be non-empty and finite. Then A has a minimum and a maximum.

Proof:

We prove that A has a maximum, the proof that A has a minimum is similar.

Suppose, with a view to obtaining a contradiction, that A has no maximum. Since $A \neq \emptyset$, $\exists\, a_0 \in A$.

Base case → Since a_0 is not a maximum, $\exists\, a_1 \in A$ s.t. $a_0 < a_1$.

Inductive step → Now, let $k \in \mathbb{N}$ and suppose $\exists\, a_1, \dots, a_k \in A$ s.t. $a_0 < a_1 < \dots < a_k$. Then, since a_k is not a maximum $\exists\, a_{k+1} \in A$ s.t. $a_k < a_{k+1}$. We conclude, by induction that $\forall n \in \mathbb{N}$ $\exists\, a_1, \dots, a_n \in A$ s.t. $a_0 < a_1 < \dots < a_n$. Hence $|A| \geq n+1$ $\forall n \in \mathbb{N}$, in particular, $|A| \geq |A|+1$, a contradiction. We conclude that A must have a maximum. □

Def^n: Let $a \in \mathbb{Z}$, we define

$$D(a) := \{ n \in \mathbb{Z} \mid n \text{ divides } a \}.$$

↑ the set of divisors of a.

Remarks:

- Every integer divides 0,
$$D(0) = \mathbb{Z}.$$
- If a is a nonzero integer then
$$d \in D(a) \Rightarrow |d| \leq |a|.$$

$a = db$, $b \in \mathbb{Z} \setminus \{0\}$ and since $|b| \geq 1$ we have $|a| \geq |d|$.

Def^n: Let a, b be integers, not both zero.

- The set of <u>common divisors</u> is defined by

$$D(a) \cap D(b) = \{n \in \mathbb{Z} \mid n \text{ divides } a \text{ and } n \text{ divides } b\}.$$

- The <u>greatest common divisor</u> of a and b is defined to be

$$\gcd(a,b) := \max\left(D(a) \cap D(b)\right).$$

Remark: When the meaning is clear from the context, $\gcd(a,b)$ will simply be denoted by (a,b).

Def^n: Let a, b be integers, not both zero. We say that a and b are <u>relatively prime</u> (or <u>coprime</u>) if $\gcd(a,b) = 1$.

$$\Updownarrow$$

$$D(a) \cap D(b) = \{-1, 1\}$$

Example: Find $\gcd(21, 56)$.

$\rightarrow$ $D(21) = \{-21, -7, -3, -1, 1, 3, 7, 21\}$

$D(56) = \{-56, -28, -14, -8, -7, -4, -2, -1, 1, 2, 4, 7, 8, 14, 28, 56\}$

So $\gcd(21, 56) = 7$.