Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 3

Translating From Mathematics to English

- Make sure you know what a question is asking before attempting it!
- Key words meaning for all: Always, Whenever, For Any, No/None.
- Key words meaning there exists: For Some, Has a, There is/is not.

1. No multiple of 15 plus any multiple of 6 equals 100.

$$\forall m, n \in \mathbb{Z}, (15m + 6n \neq 100)$$

2. $n \in \mathbb{Z} \Rightarrow (\exists m \in \mathbb{Z}, m > n)$.

   There is no greatest integer.

Contrapositive

- $H \Rightarrow C \equiv \neg C \Rightarrow \neg H$.

  Proof:

$$\begin{aligned} H \Rightarrow C &\equiv \neg H \vee C \\ &\equiv C \vee \neg H \\ &\equiv \neg(\neg C) \vee \neg H \\ &\equiv \neg C \Rightarrow \neg H. \end{aligned}$$

- $7 \nmid n \Rightarrow 14 \nmid n \equiv 14 \mid n \Rightarrow 7 \mid n$.
- Useful when you have a non existence statement or if the conclusion is the negation of an easy to use statement.

Example of Contrapositive

Example: Suppose $a, b \in \mathbb{R}$ and $ab \in \mathbb{R} - \mathbb{Q}$ (the set of irrational numbers). Show either $a \in \mathbb{R} - \mathbb{Q}$ or $b \in \mathbb{R} - \mathbb{Q}$.

Proof: Proceed by the contrapositive. Suppose that a is rational and b is rational. Then $\exists k, \ell, m, n \in \mathbb{Z}$ such that $a = \frac{k}{\ell}$ and $b = \frac{m}{n}$ with $\ell, n \neq 0$. Then

$$ab = \frac{km}{\ell n} \in \mathbb{Q}$$

as required. $\blacksquare$

Types of Implications

Let A, B, C be statements.

1. $(A \wedge B) \Rightarrow C$. These we have seen in say Divisibility of Integer Combinations or Bounds by Divisibility.
2. $A \Rightarrow (B \wedge C)$. For example:
   Let S, T, U be sets. If $(S \cup T) \subseteq U$, then $S \subseteq U$ and $T \subseteq U$.
3. $(A \vee B) \Rightarrow C$. For example
   $(x = 1 \vee y = 2) \Rightarrow x^2y + y - 2x^2 + 4x - 2xy = 2$
4. $A \Rightarrow (B \vee C)$. (Elimination)

   Example: If $x^2 - 7x + 12 \geq 0$ then $x \leq 3 \vee x \geq 4$.

   Proof: Suppose $x^2 - 7x + 12 \geq 0$ and $x > 3$. Then $0 \leq x^2 - 7x + 12 = (x-3)(x-4)$. Now, $x - 3 > 0$ and so we must have that $x - 4 \geq 0$. Hence $x \geq 4$.

Contradiction

- Generalization of Proof by Contrapositive.
- Let S be a statement. Then $S \wedge \neg S$ is false.
- Use: Assume the hypothesis is true and assume towards a contradiction that the negation of the conclusion is also true. Break math (find a statement S such that $S \wedge \neg S$ is true) and conclude that the conclusion must be true.

Example of Contradiction

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

Proof: Assume towards a contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{N}$. Assume further that a and b share no common factor (otherwise simplify the fraction first). Then $2b^2 = a^2$. Hence a is even. Write $a = 2k$ for some integer k. Then $2b^2 = a^2 = (2k)^2 = 4k^2$ and canceling a 2 shows that $b^2 = 2k^2$. Thus b^2 is even and hence b is even. This implies that a and b share a common factor, a contradiction.

Uniqueness

- To prove uniqueness, we can do one of the following:
  1. Assume $\exists x, y \in S$ such that $P(x) \wedge P(y)$ is true and show $x = y$.
  2. Argue by assuming that $\exists x, y \in S$ are distinct such that $P(x) \wedge P(y)$, then derive a contradiction.
- To prove uniqueness and existence, we also need to show that $\exists x \in S$ such that $P(x)$ is true.

Example of Uniqueness

Suppose $x \in \mathbb{R} - \mathbb{Z}$ and $m \in \mathbb{Z}$ such that $x < m < x + 1$. Show that m is unique.

Proof: Assume that $\exists m, n \in \mathbb{Z}$ such that

$$x < m < x + 1 \qquad \text{and} \qquad x < n < x + 1$$

Look at the value $m - n$. This value is largest when m is largest and n is smallest. Since $m < x + 1$ and $n > x$, we see that $m - n < 1$. Further, for this to be minimal, we could flip the roles of m and n above to see that $-1 < m - n$. Thus $-1 < m - n < 1$ and $m - n \in \mathbb{Z}$. Hence $m - n = 0$, that is $m = n$.

Injections and Surjections

Let S and T be sets. A function

$$\begin{aligned} f : S &\to T \\ x &\mapsto f(x) \end{aligned}$$

is said to be

1. Injective (or one to one or $1:1$) if and only if

$$\forall x, y \in S, f(x) = f(y) \Rightarrow x = y.$$

2. Surjective (or onto) if and only if

$$\forall y \in T\ \exists x \in S \text{ such that } f(x) = y$$

Division Algorithm

- Grade School Division.
- $51 = 7(7) + 2$
- $35 = 6(5) + 5$ and $-35 = 6(-5) - 5 = 6(-5) - 6 + 6 - 5 = 6(-6) + 1$ where $a = -35$, $b = 6$, $q = -6$, and $r = 1$.
- (Division Algorithm) Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then $\exists! q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < b$.
- Check out the proof in the notes!

Summation and Product Notation

Let $\{a_1, ..., a_n\}$ be a sequence of n real numbers. We write

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + ... + a_n.$$

We call i the index variable, 1 is the starting number, n is the upper bound. We can also write

$$\sum_{x \in S} x$$

to mean the sum of elements in S. Similarly, we define

$$\prod_{i=1}^{n} a_i := a_1 a_2 ... a_n \qquad \prod_{x \in S} := \text{ Product of elements in S}$$

We make the following conventions when $j > k$ are integers

$$\sum_{i=j}^{k} a_i = \sum_{x \in \emptyset} = 0 \qquad \text{and} \qquad \prod_{i=j}^{k} a_i = \prod_{x \in \emptyset} = 1$$

Summation and Product Notation Examples

1. $\displaystyle\sum_{i=1}^{4} i^2 = (1)^2 + (2)^2 + (3)^2 + (4)^2 = 1 + 4 + 9 + 16 = 30$
2. $\displaystyle\prod_{i=1}^{4} i^2 = (1)^2(2)^2(3)^2(4)^2 = (1)(4)(9)(16) = 576$
3. $\displaystyle\sum_{i=1}^{3.5} i = 1 + 2 + 3 = 6$
4. For $k \in \mathbb{N}$ fixed, $\displaystyle\sum_{i=k}^{2k} \frac{1}{i} = \frac{1}{k} + \frac{1}{k+1} + \dots + \frac{1}{2k}$.