16/06

~~A~~ Homework 1

0.3

6. Prove (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

a) recall: we want to show $A \subset B$ and $B \subset A$. Then,

$\Rightarrow$ Let $x \in A \cap (B \cup C)$. Then $x \in B$ or $x \in C$, and $x \in A$. If $x \in B$, then $x \in A \cap B$. So $x \in (A \cap B) \cup (A \cap C)$.

If $x \in C$, then $x \in A \cap C$. So $x \in (A \cap B) \cup (A \cap C)$.

$\Leftarrow$ Let $x \in (A \cap B) \cup (A \cap C)$. Then $x \in A \cap B$ or $x \in A \cap C$.

If $x \in A \cap B$, then $x \in A$ and $x \in B$. Then $x \in B \cup C$.

$\therefore x \in A \cap (B \cup C)$.

over union!

If $x \in A \cap C$, then $x \in A$ and $x \in C$. Then $x \in B \cup C$.

$\therefore x \in A \cap (B \cup C)$. This is the distributive law of intersection

b) $\Rightarrow$ Let $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. If $x \in A$, $x \in A \cup B$ and $x \in A \cup C$. $\therefore x \in (A \cup B) \cap (A \cup C)$.

If $x \in B \cap C \Rightarrow x \in B$ and $x \in C$. $\Rightarrow x \in (A \cup B)$ and $x \in (A \cup C)$.

$\therefore x \in (A \cup B) \cap (A \cup C)$.

$\Leftarrow$ Let $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$.

If $x \in A$, then $x \in A \cup (B \cap C)$ directly.

If $x \notin A$, then for $x \in A \cup B$ we must have $x \in B$, and for $x \in A \cup C$, we must have $x \in C$.

$\therefore x \in B \cap C$

$\therefore x \in A \cup (B \cap C)$ $\Rightarrow$ Distributive law of union over intersection!

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

$P(1)$: $1 < 2^1$, thus it holds.

$P(k)$: $k < 2^k$

Now, for $n = k+1$, We want to show $k+1 < 2^{k+1}$

$\cancel{k+1 < k+k+1 < 2k+1 < 4k+1 < 2 \cdot 2^k + 1}$

$\cancel{= 2k \cdot 2 + 1 = 2^{k+1} + 1}$

We have $k < 2k$ $\cancel{< 2^{k+1}}$

$\therefore 2k < 2k \cdot 2$

$2k < 2^{k+1}$

$k + k < 2^{k+1}$

$k+1 \leq k+k < 2^{k+1}$ $\therefore k+1 < 2^{k+1}$ $\square$

12. Show that for a finite set A of cardinality n, cardinality of $\mathcal{P}(A)$ is 2^n.

We will prove this by induction on n.

$P(0)$: If $|A| = 0$, then $A = \emptyset$

The only subset of $\emptyset$ is $\emptyset$ itself.

$\therefore \mathcal{P}(A) = \{0\} \Rightarrow |\mathcal{P}(A)| = 2^0 = 1$

$\therefore$ base case holds

Now, assume that for some $k \in \mathbb{N}$, every set of cardinality k has a power set of size 2^k. That is, for B with $|B| = k$, then $|\mathcal{P}(B)| = 2^k$.

We want to show it also holds for $k+1$.

Let $|A| = k+1$, and take an element $a \in A$. Then, we can define

$B = A \setminus \{a\} \Rightarrow |B| = k$

Now, consider how to construct the power set of A. Every subset of A either contains a or it does not.

So we can partition $\mathcal{P}(A)$ into two disjoint parts.

1. Subsets of A with no a. That is, $\mathcal{P}(B)$.
2. Subsets of A with a. That is, $\{S \cup \{a\} : S \subseteq B\}$.

$\therefore \mathcal{P}(A) = \mathcal{P}(B) \cup \{S \cup \{a\} : S \in \mathcal{P}(B)\}$

$|\mathcal{P}(B)| = 2^k$ by the inductive hypothesis

Every set $S \in \mathcal{P}(B)$ will have a one-to-one correspondence with $S \cup \{a\}$, since we are simply adding a.

$\therefore |\{S \cup \{a\} : S \in \mathcal{P}(B)\}| = 2^k$

Since the two sets are disjoint, recall, these are sets of sets, so there is no intersection

$|\mathcal{P}(A)| = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$

Thus, by induction, the statement holds for all $n \in \mathbb{N}$. $\square$

15. Prove that n^3+5n is divisible by 6 for all $n \in \mathbb{N}$.

$P(1)$: $1^3+5\cdot 1=6$ $\therefore$ $P(1)$ holds

$P(k)$: Assume k^3+5k is divisible by 6 for all $k \in \mathbb{N}$. That is,

$k^3+5k=6a$, for some $a \in \mathbb{Z}$.

We want to show it also holds for $k+1$.

$$(k+1)^3+5(k+1) = k^3+3k^2+3k+1+5k+5$$
$$= k^3+5k+3k^2+3k+6$$
$$= 6a+3k(k+1)+6$$
$$= 6a+6\left(\frac{k(k+1)}{2}\right)+6$$

$\because k(k+1)$ will always be even.

$\therefore P(k+1)$ holds.

$\therefore$ by induction, n^3+5n is divisible by 6 for all $n \in \mathbb{N}$.

19. Give an example of a countably infinite collection of finite sets $A_1, A_2, \ldots$, whose union is not a finite set.

Consider $A_n = \{d \in \mathbb{N} : d | n\}$

It is both finite and $\{A_n\}$ is countably infinite.

Now, every $m \in \mathbb{N}$ divides some natural number. $m|m, m|2m \ldots$

$$\therefore \bigcup_{n=1}^{\infty} A_n = \mathbb{N}$$

Bonus: Prove that $|\{q \in \mathbb{Q} : q > 0\}| = |\mathbb{N}|$.

We want to find a bijective function from one set to the other.

Define $f : \{q \in \mathbb{Q} : q > 0\} \to \mathbb{N}$ as follows

If $f(1) = 1$. If $q \in \mathbb{N} \setminus \{1\}$, then

$$f(q) = p_1^{2r_1} \cdots p_n^{2r_n}$$

If $q \in \mathbb{Q} \setminus \mathbb{N}$, then

$$f(q) = p_1^{2r_1} \cdots p_n^{2r_n} q_1^{2s_1 - 1} \cdots q_m^{2s_m - 1}$$

(a) Compute $f(4/15)$. Find q such that $f(q) = 108$.

$$(4/15) = \frac{2^2}{3^1 \cdot 5^1} \qquad \therefore f(4/15) = 2^4 \cdot 3^1 \cdot 5^1 = 240$$

$$108 = 2^2 \cdot 3^3 \to 2^2 \cdot 3^3 = p_1^{2r_1} \cdots p_n^{2r_n} q_1^{2s_1 - 1} \cdots q_m^{2s_m - 1}$$

$$\therefore p_1^{r_1} = 2^1 \text{ and } q_1^{s_1} = 3^2 \quad \therefore q = 2/3^2 = 2/9$$

(b) Prove that f is a bijection.

①: We want to show f is injective. That is, $f(t_1) = f(t_2) \to t_1 = t_2$

Let $f(q_1) = f(q_2)$. Then

$$p_1^{2r_1} \cdots p_n^{2r_n} = q_1^{2s_1} \cdots q_m^{2s_m}$$, where $p_1 \cdots p_n$ and $q_1, \cdots, q_m$ are unique prime numbers and $r_1 \cdots r_n$, $s_1 \cdots s_m$ are unique exponents by the fundamental theorem of arithmetic.

$\therefore f(q_1) = f(q_2)$ only if $p_1^{r_1} = q_1^{s_1}, \cdots, p_n^{r_n} = q_m^{s_m}$ $\therefore t_1 = t_2$

② : Surjective

We want to show that $\forall q \in \mathbb{Q}, q > 0, \exists n \in \mathbb{N}$ s.t. $q = p_1^{2r_1} \cdots p_n^{2r_n}$

or that $\forall n \in \mathbb{N}, \exists q \in \mathbb{Q}, q > 0$ s.t. $f(q) = n$

Let $n \in \mathbb{N}$. Then n is given by

$f(q) = p_1^{2r_1} \cdots p_n^{2r_n}$ or $f(q) = p_1^{2r_1} \cdots p_n^{2r_n} q_1^{2s_1 - 1} \, q_m^{2s_m - 1}$

The fundamental theorem of arithmetic guarantees that each

$q = p_1^{r_1} \cdots p_n^{r_n}$ or $q = p_1^{r_1} \cdots p_n^{r_n} / q_1^{s_1} \cdots q_m^{s_m}$ is unique

$\therefore$ so all of $\mathbb{N}$ gets mapped.