CSE 16 6-25-20

Recall: if $J \subseteq I$ and $J \neq \emptyset$, then

$$(*) \quad \bigcup_{\alpha \in J} A_\alpha \subseteq \bigcup_{\alpha \in I} A_\alpha$$

Proof.

Suppose $x \in \bigcup_{\alpha \in J} A_\alpha$. Then for some $\beta \in J$, $x \in A_\beta$. Since $J \subseteq I$, we have $\beta \in I$. Thus $x \in A_\beta$ for $\beta \in I$. Therefore

$$x \in \bigcup_{\alpha \in I} A_\alpha .$$

We've shown that $\bigcup_{\alpha \in J} A_\alpha \subseteq \bigcup_{\alpha \in I} A_\alpha$. ∎

each statement in a Proof should follow logically the previous state. by some

(1) definition.

(2) inference rule.

(3) Previously proved facts.

Incidentally, what is meant by

$$\bigcup_{\alpha \in I} A_\alpha \quad \text{and} \quad \bigcap_{\alpha \in I} A_\alpha$$

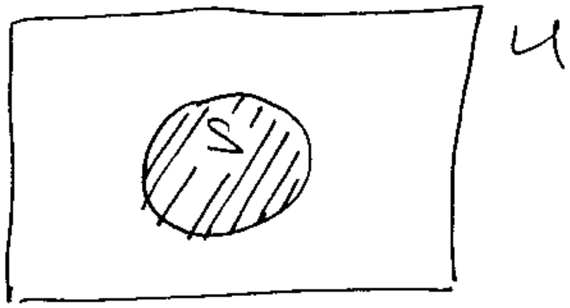
when $I = \phi$. <u>Answer</u>:

$$\bigcup_{\alpha \in I} A_\alpha = \phi \quad \text{and} \quad \bigcap_{\alpha \in I} A_\alpha = \mathcal{U}$$

note:

- $S \cup \emptyset = S$

- $S \cap U = S$ for any $S \subseteq U$



so (*) is true, even if $J = \emptyset$.

(1.9) Number Systems

Recall

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

observe that $\mathbb{N}$ has a property not shared by the others

<u>Fact</u> (well ordering Property of $\mathbb{N}$) (W.O.P.)

Any non-empty subset of $\mathbb{N}$ contains a least element.

In other words, if $A \subseteq \mathbb{N}$ and $A \neq \emptyset$, then there exists $x_0 \in A$ such that $x_0 \leq x$ for all $x \in A$.

This is not a theorem, instead its an <u>Axiom</u>, i.e. assumed to be true without proof.

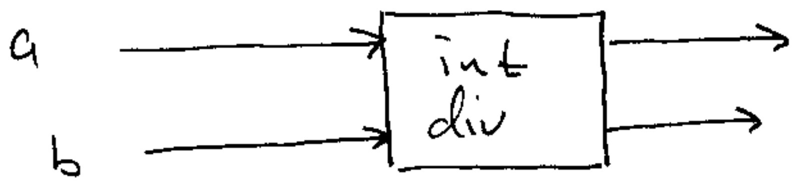
study of $\mathbb{N}$ and $\mathbb{Z}$ is called <u>number theory</u>.

<u>Theorem</u> (Division Algorithm)

Given $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \le r < b$$

dividend (a), quotient (q), divisor (b), remainder (r)



$q = a \ \underline{\text{div}}\ b = a/b$

$r = a \ \underline{\text{mod}}\ b = \underbrace{a \% b}_{\text{in C, C++, Java}}$

Two things to prove

(1) existence of q, r

(2) uniqueness of q, r

Proof of (1)

Let

$$A = \{ a - xb \mid x \in \mathbb{Z} \text{ and } 0 \le a - xb \le a \}$$

observe

$$A \subseteq \{0, 1, 2, \ldots\} = \underbrace{\{0\} \cup \mathbb{N}}$$

non-negative ints also satisfy W.O.P.

since $A \neq \phi$, it contains a least element, by W.O.P. Call it r

Thus

$$r = a - qb \quad \text{for some } q \in \mathbb{Z}$$

and

$$r \geq 0$$

observe that if $\boxed{r \geq b}$, we have

$$0 \leq r - b = (a - qb) - b$$
$$= a - (q+1)b < a - qb = r$$

we have another number of the form $a - xb$ (namely $a - (q+1)b$) that is ≥ 0 and $< r$. This is impossible since r was the <u>least</u> such number. Therefore $r \geq b$ must be false, hence $r < b$.

so

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

as required. $\blacksquare$

Exercise

Try to prove (2) uniqueness, i.e. suppose

$$a = q_1 b + r_1 \quad , \quad 0 \leq r_1 < b$$

and

$$a = q_2 b + r_2 \quad , \quad 0 \leq r_2 < b.$$

Then show $q_1 = q_2$ and $r_1 = r_2$.

John Von Neuman invented modern method for constructing 0, 1, 2, ... from sets.

Basic operation : <u>Successor</u>

$$\boxed{S^+ = S \cup \{S\}}$$

$0 = \phi$

$1 = 0^+ = 0 \cup \{0\} = \phi \cup \{0\} = \{0\}$

$2 = 1^+ = 1 \cup \{1\} = \{0, 1\}$

$3 = 2^+ = 2 \cup \{2\} = \{0, 1, 2\}$

$4 = 3^+ = 3 \cup \{3\} = \{0, 1, 2, 3\}$

$\vdots$

$n = \{0, 1, 2, \ldots, n-1\}$

$\vdots$

The collection (set)

$$\{0,1,2,\ldots\ldots\} = \{0\} \cup \mathbb{N}$$

can be shown to satisfy W.O.P.

(1.10) Russel's Paradox

can there be a set that has itself as a member?

Like

$$A = \{A\} = \{\{A\}\} = \{\{\{A\}\}\}$$
$$\vdots$$
$$= \{\{\{\{\cdots\cdots\}\}\}\}$$

The naive definition of set offers no obstacle to this set.

we can also form

$$\mathcal{S} = \{ x \mid x \text{ is a set} \}$$
$$= \{ \text{all sets} \}$$

Evidently $\mathcal{S} \in \mathcal{S}$. On the other hand $\emptyset \notin \emptyset$.

Define

$$\mathcal{R} = \{ A \in \mathcal{S} \mid A \notin A \}.$$

$\mathcal{R}$ contains the 'normal' sets, but $\mathcal{R}$ itself causes the Paradox.

clearly either $\mathcal{R} \notin \mathcal{R}$ or $\mathcal{R} \in \mathcal{R}$.

If $\mathcal{R} \in \mathcal{R}$ then $\mathcal{R}$ must satisfy the defining property of $\mathcal{R}$, namely

$$\mathcal{R} \notin \mathcal{R}$$

If $R \notin R$, then R satisfies the defining property of R, hence

$$R \in R$$

Thus $R \in R$ iff $R \notin R$, which is a paradox.

In 1931 Kurt Gödel proved no sufficiently strong mathematical system can prove its own consistency.

<u>Read chapter 2</u>. Logic