Lecture 12

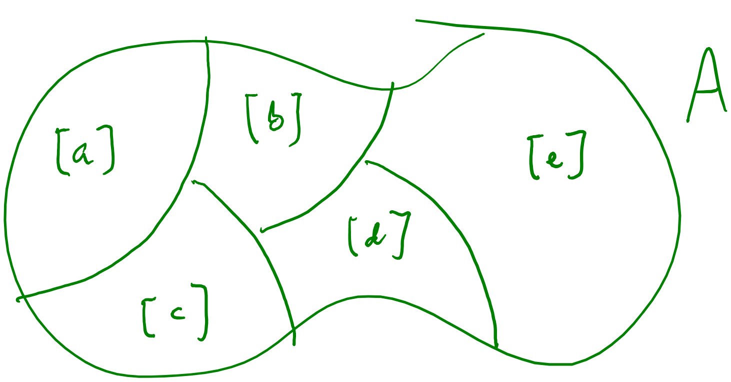
Friday, February 13, 2015 7:56 AM

Mon - Wed:
- Cartesian product $A \times B = \{(a,b) \mid a \in A, b \in B\}$
- Relations $R \subseteq A \times B$
- Equivalence relations
- Functions

$(a,b) \in R$
write aRb

Equiv rel'n on A is a rel'n on A satisfying
1. reflexivity: $\forall a \in A$. aRa
2. symmetry: if aRb, then bRa
3. transitive: if aRb and bRc, then aRc.

For $a \in A$, $[a] = [a]_R = \{ b \in A \mid aRb \}$



Friday, February 13, 2015 8:08 AM

Functions: $f : A \longrightarrow B$ is a relation on $A \& B$ such that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$.

$$[\forall a \in A .\ \exists!\, b \in B .\ (a,b) \in f]$$

Write $f(a) = b$ when $(a,b) \in f$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

$F : X \longrightarrow Y$

Injective: If $F(x) = F(x')$, then $x = x'$.

Surjective: For every $y \in Y$, there exists $x \in X$ s.t. $F(x) = y$.

Bijective: inj + surj.

(A has n elts. Injection $A \times A \longrightarrow \{\text{subsets of } A\}$ would show $n^2 \leq 2^n$.)

Prop If $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$, then

1. if f and g are injective, then $g \circ f$ is injective
2. — " — surjective, — " — surj
3. — " — bijective, — " — bij.

Pf ① If $(g\circ f)(x) = (g\circ f)(x')$, then

$$g(f(x)) = g(f(x'))$$

and since g is injective, $f(x) = f(x')$.

Now since f is injective, $x = x'$.

Thus $g\circ f$ is injective.

② To check that $g\circ f$ is surjective, for each $z \in Z$ we must show there is $x \in X$ such that

$$(g\circ f)(x) = z.$$

Take $z \in Z$. Since g is surjective, there exists $y \in Y$ s.t. $g(y) = z$. Since f is surjective, there exists $x \in X$ s.t. $f(x) = y$. Now

$$(g\circ f)(x) = g(f(x)) = g(y) = z,$$

as desired.

③ Follows from ① & ②. $\square$

Binary operations

Defn A binary operation on a set A $\square$ is a function $\square : A \times A \to A$.

Notation $\square((a,b)) = \square(a,b) = a \square b$.

e.g. ① On $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots,$ addition $(\square = +)$ and multiplication $(\square = \cdot)$ are binary ops.

② Subtraction $(\square = -)$ is a binary op on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, but not on $\mathbb{N}$ (codomain too small!)

③ Division $(\square = \div)$ is a binary op on $\mathbb{Q} - \{0\}$, $\mathbb{R} \setminus \{0\}$, $\{1, -1\}$.

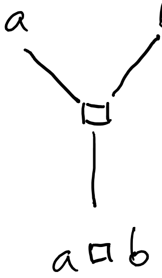
Defn For a set A, let $\mathcal{P}(A) = \{\text{subsets of } A\}$. $\mathcal{P}(A)$ is the power set of A.

④ $\cap, \cup, \setminus$ are binary ops on $\mathcal{P}(A)$

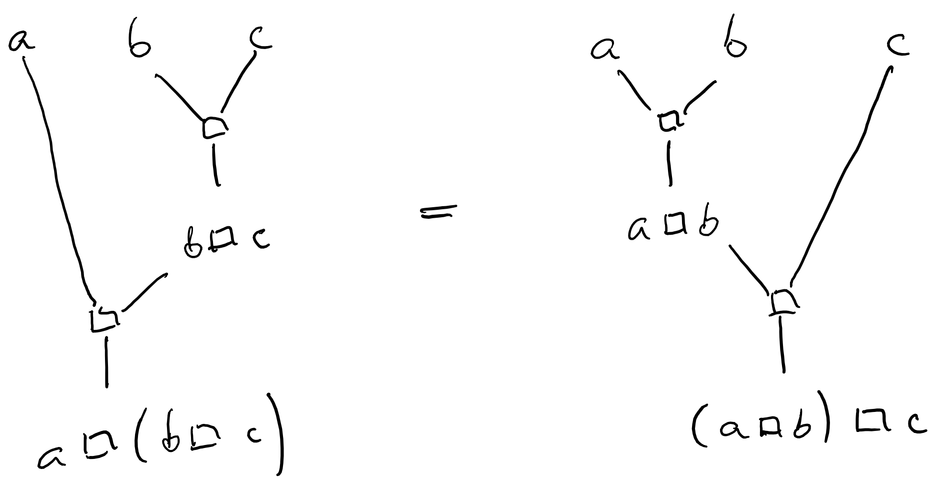
⑤ $\wedge, \vee$ are binary ops on statements.

Friday, February 13, 2015 8:41 AM

Think of binary ops as having 2 inputs and one output:



<u>Defn</u> A binary op $\square$ on A is <u>associative</u> if for every $a, b, c \in A$, $a \square (b \square c) = (a \square b) \square c$.



<u>e.g.</u> $+, \cdot$ are associative

$-$: $a - (b - c) \cancel{\overset{?}{=}} (a - b) - c$

$\quad \| $

$a - b + c$

Subtraction is <u>not</u> associative.