09312 — Algebra III — 1978 (2).

July 1978

§1. Sets and functions.

What is a real number? In a first course on analysis we are told that the real numbers form a complete ordered field and not to worry too much about what they really "are". If necessary we are told to keep decimal expansions in the back of our minds. This is a little unsatisfactory since our intuition is stretched when we try to make decimals form a field: for example, how do we multiply two infinite non-recurring decimals?

At present algebra is couched in the language of sets with structure. What is a set? In early life we are told that sets are collections of things called elements. Some properties of intersections, unions, complements, functions, &c, are then "proved". No attempt is made at that stage to characterize all sets in the way that the complete ordered field properties characterize all real numbers.

It is possible to so axiomatize sets. Furthermore it is possible to do it in a spirit consistent with that of algebra so that light is thrown on the basic constructions of algebra in their barest form: constructions for sets. The position with sets is even more satisfactory than with decimals in that collections of elements intuitively satisfy the axioms.

The data for a complete ordered field you will recall are:

symbols $a, b, c, x, y, \ldots$ called real numbers certain of which are distinguished and called positive and two of which are denoted by $0, 1$;

for each pair of real numbers a, b, real numbers $a+b$, $a \times b$;

for each real number a, a real number $-a$, and, for $a \neq 0$, a real number $1/a$;

and these data are asked to satisfy a long list of axioms.

We shall now develop such an axiomatic approach to sets.

The data are as follows:

D1. symbols $A, B, C, X, Y, \ldots$ called sets;

D2. symbols $f, g, u, v, \ldots$ called functions;

D3. for each function f, a set A called the domain of f and a set B called the codomain of f which we express in the notation $f : A \to B$ or $A \xrightarrow{f} B$;

D4. for each set A, a function $1_A : A \to A$ called the identity of A;

D5. for each pair of functions f, g such that the domain of g is the codomain of f, a function gf, called <u>the composite of</u> f, g, whose domain is the domain of f and whose codomain is the codomain of g.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "gf"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

These data are to satisfy axioms which we state below. We shall not give them all at once, but rather intersperse them with various definitions, logical consequences (theorems), and intuitive connections to collections of things. The last are not necessary for the formal development.

<u>Ax. 1.</u> <u>For all functions</u> $f : A \to B$, $\quad 1_B f = f = f 1_A$.

<u>Ax. 2.</u> <u>For all functions</u> $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$,
$(hg)f = h(gf)$.

A function $r : A \to B$ is called a <u>retraction</u> when there exists a function $i : B \to A$ such that $ri = 1_B$.

A function $m : B \to A$ is called a <u>coretraction</u> when there exists a function $e : A \to B$ such that $em = 1_B$.

A function $m : B \to A$ is called <u>monic</u>

when, for all functions $C \overset{u}{\underset{v}{\rightrightarrows}} B$, if $mu = mv$ then $u = v$. Write $m: B \rightarrowtail A$ to mean m monic.

A function $e: A \to B$ is called <u>epic</u> when, for all functions $B \overset{h}{\underset{k}{\rightrightarrows}} D$, if $he = ke$ then $h = k$. Write $e: A \twoheadrightarrow B$ to mean e epic.

<u>Theorem 1</u>. <u>Each retraction is epic. Each coretraction is monic.</u>

<u>Proof</u>. Suppose $em = 1_B$ and $mu = mv$. Then $u = 1_B u = (em)u = e(mu) = e(mv) = (em)v = 1_B v = v$. So coretractions are monic. The other statement is similar. □

A function $f: A \to B$ is called an <u>isomorphism</u> when it is both a retraction and a coretraction.

<u>Theorem 2</u>. <u>The following statements about a function</u> $f: A \to B$ <u>are equivalent</u>:

(a) f <u>is an isomorphism</u>;

(b) <u>there exists a unique function</u> $f^{-1}: B \to A$ <u>such that</u> $ff^{-1} = 1_B$, $f^{-1}f = 1_A$;

(c) f <u>is a monic and a retraction</u>;

(d) f <u>is an epic and a coretraction</u>.

<u>Proof</u>. (a) ⇒ (b) Suppose f is an isomorphism so that $fh = 1_B$, $kf = 1_A$ for some h, k. Then $h = 1_A h = (kf)h = k(fh) = k1_B = k$. So $h = f^{-1}$ has the property required in (b). (b) ⇒ (c) Assuming (b), we have that f is a coretraction and a retraction. So (c) follows

from Theorem 1.

(c)$\Rightarrow$(d) Suppose f monic and $fh = 1_B$. Then $f(hf) = (fh)f = 1_B f = f = f1_A$. Since f is monic, $hf = 1_A$. So f is a coretraction. But f is epic by Theorem 1. So (d) holds.

(d)$\Rightarrow$(a) A similar argument shows f epic and coretraction imply f retraction. So f isomorphism. $\square$

For an isomorphism $f: A \to B$, call f^{-1} the <u>inverse</u> of f. Two sets A, B are said to be <u>isomorphic</u> when there exists an isomorphism $f: A \to B$. In this case we write $A \cong B$.

Clearly identities are isomorphisms, a composite of isomorphisms is an isomorphism $(gf)^{-1} = f^{-1}g^{-1}$, and the inverse of an isomorphism is an isomorphism. So we have:

$$A \cong A, \quad A \cong B \Rightarrow B \cong A, \quad \text{and } A \cong B, B \cong C \Rightarrow A \cong C.$$

<u>Ax. 3.</u> <u>There is a set 1 such that, for all sets A, there is precisely one function $A \to 1$.</u>

<u>Theorem 3.</u> <u>Suppose T is a set for which, for all sets A, there is precisely one function $A \to T$. Then $T \cong 1$ by a unique isomorphism.</u>

<u>Proof.</u> The properties of $T, 1$ supply unique functions $1 \to T$, $T \to 1$. The composite $1 \to T \to 1$ must be 1_1 since there is only one function $1 \to 1$. Similarly $T \to 1 \to T$ is 1_T. So $1 \to T$ is inverse for $T \to 1$. $\square$

We think of 1 as the set with precisely one element.

In fact, define an <u>element</u> of a set A to be a function $a : 1 \to A$. Write $a \in A$ in this case. Then indeed 1 does have precisely one element.

Suppose $f : A \to C$, $g : B \to C$ are functions. <u>A pullback of</u> f, g is a set P together with functions $p_1 : P \to A$, $p_2 : P \to B$ such that $f p_1 = g p_2$, and the further property that, for all sets X and functions $u : X \to A$, $v : X \to B$ such that $fu = gv$, there exists a unique function $w : X \to P$ such that $p_1 w = u$, $p_2 w = v$. Since w is uniquely determined by u, v, we denote it by $\binom{u}{v}$.

$$\begin{tikzcd}
X \arrow[dr, dashed, "\binom{u}{v}"'] \arrow[drr, bend left, "v"] \arrow[ddr, bend right, "u"'] & & \\
& P \arrow[r, "p_2"] \arrow[d, "p_1"'] & B \arrow[d, "g"] \\
& A \arrow[r, "f"'] & C
\end{tikzcd}$$

In other words, functions $w : X \to P$ are determined by pairs of functions $u : X \to A$, $v : X \to B$ such that $fu = gv$. In particular, we see that, by taking $X = 1$, elements of P amount to pairs of elements $a \in A$, $b \in B$ such that $fa = gb$. Call p_1, p_2 <u>projections</u>.

Our intuition allows us to form, from the functions f, g, the set

$$P = \left\{ \binom{a}{b} \;\middle|\; a \in A,\ b \in B,\ fa = gb \right\}$$

and the functions p_1, p_2 given by $p_1\binom{a}{b}=a$, $p_2\binom{a}{b}=b$. This does in fact give a pullback of f, g since $f p_1 = g p_2$; and, given u, v with $fu = gv$, we are forced to define $wx = \binom{ux}{vx}$ if we want $p_1 w = u$, $p_2 w = v$.

<u>Ax. 4</u>. <u>Each pair of arrows with the same codomain has a pullback.</u>

The same sort of argument as given in the proof of Theorem 3 yields:

<u>Theorem 4</u>. <u>Any two pullbacks of the same pair of functions are isomorphic by a unique isomorphism which is compatible with the projections.</u> $\square$

For sets A, B, a pullback of $A \to 1 \leftarrow B$ is denoted by $A \xleftarrow{p_1} A\times B \xrightarrow{p_2} B$ and called a <u>product</u> of A, B. A function $w : X \to A\times B$ is completely determined by two functions $u : X \to A$, $v : X \to B$ via the equations $p_1 w = u$, $p_2 w = v$.

Given functions $A \underset{k}{\overset{h}{\rightrightarrows}} B$, we can form a pullback

$$\begin{tikzcd} E \arrow[r] \arrow[d, "m"'] & B \arrow[d, "\binom{1_B}{1_B}"] \\ A \arrow[r, "\binom{h}{k}"'] & B\times B . \end{tikzcd}$$

The function $m : E \to A$ is called an <u>equalizer</u> of h, k. Notice that $hm = km$ (the common value is the function $E \to B$ at the top of the above square), and, if $u: X \to A$ is such that $hu = ku$, then there exists a unique function $w: X \to E$ such that $u = mw$. In other words, m is the universal function into A which renders h, k equal. The elements of E are determined by an element a of A for which $ha = ka$.

So far the only set we are sure exists is 1. The next axiom introduces what should be thought of as the set 2 with two elements β, τ. The existence of a set with precisely two elements is not a very powerful assertion. The fundamental property that 2 has is that functions $A \to 2$ into 2 correspond to "subsets" of A.

Ax. 5. There exist a set 2 and an element $\tau: 1 \to 2$ such that, for all monics $m: A \rightarrowtail B$, there exists a unique function $\chi_m : B \to 2$ such that ~~the~~ $1 \leftarrow A \overset{m}{\rightarrowtail} B$ is a pullback for τ, χ_m.

$$\begin{tikzcd} A \arrow[r] \arrow[d, tail, "m"'] \arrow[dr, phantom, "\text{p.b.}"] & 1 \arrow[d, "\tau"] \\ B \arrow[r, "\chi_m"'] & 2 \end{tikzcd}$$

Theorem 5. A function is monic if and only if it is an equalizer of a pair of functions.

Proof. Suppose $m: A \to B$ is an equalizer of h, k, and suppose $mu = mv$. Then $hmu = kmu$. By the property of equalizers, there exists a unique w such that $mw = mu$. But u, v both have this property of w. So $u = v = w$. So m is a monic.

If m is a monic then, from the pullback square above, we see easily that m is an equalizer of χ_m and the composite $A \to 1 \xrightarrow{\tau} 2$. $\square$

Theorem 6. *A function is an isomorphism if and only if it is epic and monic.*

Proof. By Theorems 1, 2, if f is an isomorphism then it is epic and monic. Suppose $f : A \to B$ is epic and monic. By Theorem 5, f is an equalizer of some $h, k : B \to C$. So $hf = kf$. Since f is epic this implies $h = k$. So $h 1_B = k 1_B$. So there exists a unique $w : B \to A$ such that $fw = 1_B$. So f is a retraction. By Theorem 2, f is an isomorphism. $\square$

Theorem 7. *Suppose in the following diagram that $mu = ve$, m is monic, and e is epic. Then there exists a unique function w such that $mw = v$, $we = u$.*

$$\begin{tikzcd}
A \arrow[r, two heads, "e"] \arrow[d, "u"'] & B \arrow[d, "v"] \arrow[dl, dashed, "w"'] \\
C \arrow[r, tail, "m"'] & D
\end{tikzcd}$$

Proof. By Theorem 5, m is an equalizer of h, k, say. Thus $hve = hmu = kmu = kve$, and e is epic; so $hv = kv$. By the property of equalizers, there exists a unique w such that $mw = v$. But then $mwe = ve = mu$ and m is monic, so $we = u$. $\square$

Ax. 6. *For each set A, there exists a set $\wp A$ and a function $\varepsilon_A : \wp A \times A \longrightarrow 2$ such that, for all functions $f : C \times A \longrightarrow 2$, there exists a unique function $g : C \longrightarrow \wp A$ such that* $f = \varepsilon_A \binom{g p_1}{p_2}$.

$$\begin{tikzcd} \wp A \times A \arrow[r, "\varepsilon_A"] & 2 \\ C \times A \arrow[u, "\binom{g p_1}{p_2} = g \times 1_A"] \arrow[ur, "f"'] & \end{tikzcd}$$

Note the following two facts about products. The projection $1 \times A \longrightarrow A$ is an isomorphism. Functions $u : A \longrightarrow B$, $v : C \longrightarrow D$ induce a function $u \times v = \binom{u p_1}{v p_2} : A \times C \longrightarrow B \times D$.

To see more intuitively what $\wp A$ is, we look at its elements. By Ax. 6, an element $1 \longrightarrow \wp A$ is determined by a function $1 \times A \longrightarrow 2$; that is, a function $A \longrightarrow 2$. Such functions are characteristic functions of "subsets" of A. So $\wp A$ is the "set of subsets of A".

We call $\wp A$ the *power set* of A.

A relation from A *to* B consists of a set R and functions $q_1 : R \longrightarrow A$, $q_2 : R \longrightarrow B$ such that $\binom{q_1}{q_2} : R \longrightarrow A \times B$ is monic. By abuse of language we shall often just write R for the relation and use the same symbols q_1, q_2 for all relations. This is only confusing in the case where we wish to regard the same R together with q_2, q_1 as a relation from B to A; so in this case we write R° for the relation from B to A called the <u>reverse</u> of R.

For functions $a : X \to A$, $b : X \to B$, we write bRa when there exists a function $x : X \to R$ such that $q_1 x = a$, $q_2 x = b$. Since $\binom{q_1}{q_2}$ is monic, such an x is unique if it exists. We say a, b are R-<u>related</u> in this case.

Suppose R, S are relations from A to B. Write $R \leq S$ when $q_1 : R \to A$, $q_2 : R \to B$ are S-related. We say R, S are <u>isomorphic relations</u> when $R \leq S$ and $S \leq R$. This amounts to saying there exists an isomorphism $f : R \to S$ such that $q_1 f = q_1$, $q_2 f = q_2$.

$$\begin{tikzcd} & R \arrow[dl, "q_1"'] \arrow[dr, "q_2"] \arrow[dd, "f", "\cong"'] & \\ A & & B \\ & S \arrow[ul, "q_1"] \arrow[ur, "q_2"'] & \end{tikzcd}$$

For each set A, we define the <u>membership relation</u> $\in_A$ from $\wp A$ to A by the pullback:

$$\begin{tikzcd} \in_A \arrow[r] \arrow[d, "\binom{q_1}{q_2}"'] \arrow[dr, phantom, "p.b."] & 1 \arrow[d, "\tau"] \\ \wp A \times A \arrow[r, "\varepsilon_A"'] & 2 \end{tikzcd}$$

It follows from the exercises that τ and hence $\binom{q_1}{q_2}$ are monic.

Theorem 8. For each relation R from A to B, there exists a unique function $r : A \to 8B$ such that there is a pullback:

$$\begin{tikzcd} R \arrow[r] \arrow[d, "\binom{q_1}{q_2}"'] \arrow[dr, phantom, "p.b."] & \in_B \arrow[d, "\binom{q_1}{q_2}"] \\ A\times B \arrow[r, "r\times 1_B"'] & 8B\times B . \end{tikzcd}$$

Two relations R, S from A to B are isomorphic if and only if their corresponding functions $A \to 8B$ are equal.

Proof. By Ax. 5 there is a unique function $\chi_{\binom{q_1}{q_2}} : A\times B \to 2$ such that:

$$\begin{tikzcd} R \arrow[r] \arrow[d, "\binom{q_1}{q_2}"'] \arrow[dr, phantom, "p.b"] & 1 \arrow[d, "\tau"] \\ A\times B \arrow[r, "\chi_{\binom{q_1}{q_2}}"'] & 2 . \end{tikzcd}$$

By Ax. 6 there is a unique function $r : A \to 8B$ such that $\chi_{\binom{q_1}{q_2}} = \varepsilon_B (r\times 1_B)$.

$$\begin{tikzcd} R \arrow[r, dashed] \arrow[d, "\binom{q_1}{q_2}"'] & \in_B \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & 1 \arrow[d, "\tau"] \\ A\times B \arrow[r, "r\times 1_B"'] & 8B\times B \arrow[r, "\varepsilon_B"'] & 2 \end{tikzcd}$$

The pullback property of the right-hand square above yields the function indicated by the

the relation and use the same symbols q_1, q_2 for all relations. This is only confusing when we wish to regard the same R together with q_2, q_1 as a relation from B to A; so in this case we write R° for the relation from B to A called the <u>reverse</u> of R.

For functions $a : X \to A$, $b : X \to B$, write $a R b$, and say a <u>is</u> R-<u>related to</u> b, when there exists a function $x : X \to R$ with $q_1 x = a$, $q_2 x = b$.

$$aRb : \quad \begin{tikzcd} & X \arrow[dl, "a"'] \arrow[dr, bend left, "b"] \arrow[d, dashed, "x"] & \\ A & & B \\ & R \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Suppose R, S are relations from A to B. Write $R \leq S$ when $q_1 : R \to A$, $q_2 : R \to B$ are S-related. This is equivalent to saying

$$aRb \quad \text{implies} \quad aSb.$$

We say R, S are <u>isomorphic relations</u> when $R \leq S$ and $S \leq R$. This is equivalent to saying

$$aRb \quad \text{iff} \quad aSb.$$

For each set A, define the <u>membership relation</u> $\in_A$ from A to $\mathcal{P}A$ by the pullback

$$
\begin{tikzcd}
\in_A \arrow[r] \arrow[d, "\begin{bmatrix} q_2 \\ q_1 \end{bmatrix}"'] & 1 \arrow[d, "\tau"] \\
\wp A \times A \arrow[r, "\varepsilon_A"'] & 2
\end{tikzcd}
$$

Theorem 8. *For each relation* R *from* A *to* B, *there exists a unique function* $r : A \to \wp B$ *such that*

$$a \, R \, b \quad \textit{iff} \quad b \in_B (r a).$$

Two relations R, S *from* A *to* B *are isomorphic if and only if their corresponding functions* $A \to \wp B$ *are equal.*

dotted arrow. The left-hand square is a pullback by one of the exercises since the outside and the right-side are pullbacks. Thus we have an r with the desired property. Uniqueness and the second statement in the theorem are left to the reader. $\square$

Notice that the pullback of the above theorem can be rewritten as a diagram:

$$\begin{tikzcd} R \arrow[r] \arrow[d, "q_1"'] \arrow[rr, bend left, "q_2"] \arrow[dr, phantom, "\text{p.b.}"] & \in_B \arrow[r, "q_2"'] \arrow[d, "q_1"] & B \\ A \arrow[r, "r"'] & \mathcal{P}B & \end{tikzcd} .$$

Intuitively, for $a \in A$, ra is the subset of B consisting of those $b \in B$ such that bRa.

Define <u>a subset of</u> B to be an element of $\mathcal{P}B$. A subset x of B gives rise to a genuine set via the pullback:

$$\begin{tikzcd} X \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{p.b.}"] & \in_B \arrow[d, "q_1"] \\ 1 \arrow[r, "x"'] & \mathcal{P}B \end{tikzcd}$$

The composite $X \longrightarrow \in_B \xrightarrow{q_2} B$ is then a monic. Monics into B give rise to subsets of B; two monics give rise to the same subset if and only if they are isomorphic (as relations from 1 to B).

For relations R, R' from A to B, we obtain a new relation $R \cap R'$ from A to B from the pullback:

$$\begin{tikzcd} R \cap R' \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & R' \arrow[d, tail, "\binom{q_1}{q_2}"] \\ R \arrow[r, tail, "\binom{q_1}{q_2}"'] & A \times B . \end{tikzcd}$$

Theorem 9. There is a function $\cap : \mathcal{P}B \times \mathcal{P}B \longrightarrow \mathcal{P}B$ such that, if R, R' are relations corresponding to functions $r, r' : A \longrightarrow \mathcal{P}B$ (Theorem 8), then $R \cap R'$ corresponds to $\cap \binom{r}{r'} : A \longrightarrow \mathcal{P}B$.

Proof. Form the pullback:

$$\begin{tikzcd} M \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & \in_B \arrow[d, "q_2"] \\ \in_B \arrow[r, "q_2"'] & B , \end{tikzcd}$$

and observe that the three functions $q_1 p_1 : M \longrightarrow \mathcal{P}B$, $q_1 p_2 : M \longrightarrow \mathcal{P}B$, $q_2 p_1 : M \longrightarrow B$ determine a monic $M \rightarrowtail \mathcal{P}B \times \mathcal{P}B \times B$. So M is a relation from $\mathcal{P}B \times \mathcal{P}B$ to B. By Theorem 8, M corresponds to a function $\mathcal{P}B \times \mathcal{P}B \longrightarrow \mathcal{P}B$ which we denote by $\cap$.

From Theorem 8 we see that there are functions $R \longrightarrow \in_B$, $R' \longrightarrow \in_B$. These compose with $R \cap R' \longrightarrow R$, $R \cap R' \longrightarrow R'$ to yield two functions $R \cap R' \rightrightarrows \in_B$ which are made equal by $q_2 : \in_B \longrightarrow B$. So there exists a unique function $R \cap R' \longrightarrow M$ which composes with p_1, p_2 to yield $R \cap R' \rightrightarrows \in_B$. What we must show is that the following square is a pullback.

$$\begin{tikzcd} R\cap R' \arrow[r] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & M \arrow[d, "q_1"] \\ A \arrow[r, "\binom{r}{r'}"'] & \mathcal{P}B\times\mathcal{P}B \end{tikzcd}$$

To see this, suppose that we have a square

$$\begin{tikzcd} X \arrow[r, "v"] \arrow[d, "u"'] & M \arrow[d, "q_1 = \binom{q_1 p_1}{q_1 p_2}"] \\ A \arrow[r, "\binom{r}{r'}"'] & \mathcal{P}B\times\mathcal{P}B \end{tikzcd}$$

such that $\binom{r}{r'}u = p_1 v$. It follows that we have:

$$\begin{tikzcd} X \arrow[r, "p_1 v"] \arrow[d, "u"'] & \in_B \arrow[d, "q_1"] \\ A \arrow[r, "r"'] & \mathcal{P}B \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "p_1 v"] \arrow[d, "u"'] & \in_B \arrow[d, "q_1"] \\ A \arrow[r, "r'"'] & \mathcal{P}B \end{tikzcd}$$

in which $ru = q_1 p_1 v$, $r'u = q_1 p_1 v$. So there exist unique functions $X \to R$, $X \to R'$ which compose with the monics into $A\times B$ to yield $\binom{u}{q_2 p_1 v} : X \to A\times B$. Thus we obtain $X \to R\cap R'$. Uniqueness is easily checked. $\square$

For $r, r' : A \to \mathcal{P}B$, write $r \leq r'$ when the corresponding relations R, R' are such that $R \leq R'$. This is easily seen to amount to the condition that the relations R, $R\cap R'$ should be isomorphic. By Theorem 9 we have that:

$$r \leq r' \text{ if and only if } r = \cap\binom{r}{r'}.$$

Clearly, for $a : X \to A$, if $r \leq r'$ then $ra \leq r'a$.

Theorem 10. *Suppose* $r : A \to 8B$, $s : C \to 8B$ *correspond to relations* R, S. *There is a relation* $R \downarrow S$ *from* A *to* C *such that, in the diagram*

$$\begin{tikzcd} R\downarrow S \arrow[r, "q_2"] \arrow[d, "q_1"'] & C \arrow[d, "s"] \\ A \arrow[r, "r"'] & 8B, \end{tikzcd}$$

$rq_1 \leq sq_2$, *and, for all diagrams*

$$\begin{tikzcd} X \arrow[r, "v"] \arrow[d, "u"'] & C \arrow[d, "s"] \\ A \arrow[r, "r"'] & 8B \end{tikzcd}$$

with $ru \leq sv$, *there exists a unique* $w : X \to R\downarrow S$ *such that* $q_1 w = u$, $q_2 w = v$.

Proof. Define $R\downarrow S$ to be the equalizer

$$R\downarrow S \rightarrowtail A\times C \underset{\cap(r\times s)}{\overset{rp_1}{\rightrightarrows}} 8B$$

and note that

$$\begin{aligned} & rp_1\binom{u}{v} = \cap(r\times s)\binom{u}{v} \\ \Leftrightarrow \quad & ru = \cap\binom{ru}{sv} \\ \Leftrightarrow \quad & ru \leq sv. \quad \square \end{aligned}$$

In particular, we obtain the inclusion relation $\supset\, = \in_B \downarrow \in_B$ from $8B$ to $8B$ (or on $8B$) by taking $r = s = 1_{8B} : 8B \to 8B$. For subsets x, y of B, we have $y \supset x$ if and only if $x \leq y$.

The function corresponding to the relation $\supset$ from $\mathcal{P}B$ to $\mathcal{P}B$ is denoted by

$$\underline{up} : \mathcal{P}B \longrightarrow \mathcal{P}\mathcal{P}B$$

(given intuitively by $\underline{up}\, X = \{ Y \subset B \mid X \subset Y \}$).

The relation $R \downarrow S$ is intuitively described by:

$c(R\downarrow S)a$ when, for all $b \in B$, bRa implies bSc.

The next result makes this precise.

<u>Theorem 11. Given a relation R from A to B, a relation S from C to B, and the diagram</u>:

$$\begin{tikzcd}
P \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & R \arrow[r, "q_2"] \arrow[d, "q_1"] & B \\
K \arrow[r, "a"'] \arrow[d, "c"'] & A & \\
C & &
\end{tikzcd},$$

$c(R\downarrow S)a$ <u>if and only if</u> $q_2 p_2 \, S \, c p_1$.

<u>Proof</u>. Form the pullback

$$\begin{tikzcd}
Q \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & S \arrow[r, "q_2"] \arrow[d, "q_1"] & B \\
K \arrow[r, "c"'] & C &
\end{tikzcd}.$$

If r, s correspond to R, S, it is easily seen that:

$K \xrightarrow{a} A \xrightarrow{r} \mathcal{P}B$ corresponds to $\binom{p_1}{q_2 p_2} : P \rightarrowtail K \times B$,

and $K \xrightarrow{c} C \xrightarrow{s} \mathcal{P}B$ corresponds to $\binom{p_1}{q_2 p_2} : Q \rightarrowtail K \times B$.

By Theorem 10, $c(R\downarrow S)a$ precisely when $ra \leq sc$:

$$\begin{tikzcd}
K \arrow[r, "c"] \arrow[d, "a"'] \arrow[dr, phantom, "\leq"] & C \arrow[d, "s"] \\
A \arrow[r, "r"'] & \mathcal{P}B
\end{tikzcd}.$$

This holds precisely when $P \leq Q$ as relations from K to B; that is, when there is a function $f : P \to Q$ such that

$$\begin{tikzcd}
 & P \arrow[dl, "p_1"'] \arrow[dr, "q_2 p_2"] \arrow[d, "f"] & \\
K \arrow[r, phantom, "="] & Q \arrow[l, "p_1"] \arrow[r, "q_2 p_2"'] \arrow[r, phantom, "="] & B .
\end{tikzcd}$$

By the pullback property of Q this occurs when there is a function $h : P \to S$ such that

$$\begin{tikzcd}
 & & P \arrow[dll, "p_1"'] \arrow[drr, "p_2"] \arrow[d, "h"] & & \\
K \arrow[dr, "c"'] & = & S \arrow[dl, "q_1"] \arrow[dr, "q_2"'] & = & R \arrow[dl, "q_2"] \\
 & C & & B & ;
\end{tikzcd}$$

that is, when $q_2 p_2 \, S \, c p_1$. □

Notice in the particular case where T is a relation from A to C (replacing K in the above theorem) the result amounts to:

$$T \leq R \downarrow S \text{ if and only if } q_2 p_2 \, S \, q_2 p_1$$

Theorem 12. $T \leq R \downarrow S$ *if and only if* $R \leq T \downarrow S^{\circ}$.

Proof. $T \leq R \downarrow S \Leftrightarrow q_2 p_2 \, S \, q_2 p_1 \Leftrightarrow q_2 p_1 \, S^{\circ} \, q_2 p_2 \Leftrightarrow R \leq T \downarrow S^{\circ}$ by two applications of Theorem 11. □

For any set A we have *the singleton function* $\mathrm{sing}_A : A \to \mathcal{P}A$ which corresponds to the relation $\binom{1_A}{1_A} : A \to A \times A$ from A to A.

Theorem 13. *The function* $\bigcap : \mathcal{P}\mathcal{P}B \to \mathcal{P}B$ *corresponding to the relation* $\in_{\mathcal{P}B} \downarrow \in_B$ *from* $\mathcal{P}\mathcal{P}B$ *to* B *has the following properties:*

(i) $r \leq \bigcap f$ *if and only if* $f \leq \mathrm{up}_A \, r$

(ii) if $u, v : A \to \mathcal{P}B$ are such that $u \leq v$ then $\bigcap v \leq \bigcap u$;

(iii) $\bigcap \underline{\text{sing}}_{\mathcal{P}B} = 1_{\mathcal{P}B} = \bigcap \underline{\text{up}}$.

Proof. (i) Let R, F be the relations corresponding to $r : A \to \mathcal{P}B$, $f : A \to \mathcal{P}\mathcal{P}B$. Then $R{\downarrow}\in_B$, $F{\downarrow}\in_B^{\circ}$ correspond to $\underline{\text{up}}\, r : A \to \mathcal{P}\mathcal{P}B$, $\bigcap f : A \to \mathcal{P}B$ (Theorem 10). By Theorem 12,

$$r \leq \bigcap f \iff R \leq F{\downarrow}\in_B^{\circ} \iff F \leq R{\downarrow}\in_B \iff f \leq \underline{\text{up}}\, r.$$

(ii) By (i), $\bigcap v \leq \bigcap v$ implies $v \leq \underline{\text{up}} \bigcap v$. So $u \leq \underline{\text{up}} \bigcap v$. So by (i), $\bigcap v \leq \bigcap u$.

(iii) Let Δ denote the relation $\binom{1_{\mathcal{P}B}}{1_{\mathcal{P}B}} : \mathcal{P}B \to \mathcal{P}B \times \mathcal{P}B$ so that $\bigcap \underline{\text{sing}}_{\mathcal{P}B}$ corresponds to $\Delta{\downarrow}\in_B^{\circ}$. Applying Theorem 12 to the diagram

$$\begin{tikzcd}
R \arrow[r, "q_1"] \arrow[d, "1_R"'] \arrow[dr, phantom, "\text{p.b.}"] & \mathcal{P}B \arrow[r, "1_{\mathcal{P}B}"] \arrow[d, "1_{\mathcal{P}B}"] & \mathcal{P}B \\
R \arrow[r, "q_1"'] \arrow[d, "q_2"'] & \mathcal{P}B & \\
B & &
\end{tikzcd}$$

we see that $R \leq \Delta{\downarrow}\in_B^{\circ}$ if and only if $R \leq \in_B$. Taking $R = \in_B$ gives $\in_B \leq \Delta{\downarrow}\in_B^{\circ}$. Taking $R = \Delta{\downarrow}\in_B^{\circ}$ gives $\Delta{\downarrow}\in_B^{\circ} \leq \in_B$. So the functions $\mathcal{P}B \to \mathcal{P}B$ corresponding to $\Delta{\downarrow}\in_B^{\circ}$, $\in_B$ are equal. ~~So $\bigcap \underline{\text{sing}} = 1$.~~ The other part is left to the reader. $\square$

<u>Universal quantification along a relation</u> R from A to B is the function $\forall_R : \mathcal{P}A \to \mathcal{P}B$ corresponding to the relation $(R^{\circ}{\downarrow}\in_A)^{\circ}$ from $\mathcal{P}A$ to B. (Intuitively, for $X \subset A$, $\forall_R X = \{b \in B \mid a \in X \text{ for all } a \in A \text{ with } bRa\}$.)

Two particular cases of this are important. For a function $f : A \to B$, the relation from A to B determined by the monic $\binom{1_A}{f} : A \to A \times B$ is called <u>the graph of</u> f and denoted by Γf.

We write $\forall_f : \mathcal{P}A \to \mathcal{P}B$ for $\forall_{\Gamma f}$ and call it *universal quantification along* f. ($\forall_f X = \{b \in B \mid a \in X$ for all $a \in A$ with $fa = b\}$.) We write $f^* : \mathcal{P}B \to \mathcal{P}A$ for $\forall_{(\Gamma f)^\circ}$ and call it the *inverse image function for* f. ($f^* Y = \{a \in A \mid fa \in Y\}$.)

Theorem 14. For all $f : A \to B$, the relation P from $\mathcal{P}B$ to A corresponding to $f^* : \mathcal{P}B \to \mathcal{P}A$ is given by the pullback

$$\begin{tikzcd} P \arrow[r] \arrow[d, "\binom{q_1}{q_2}"'] \arrow[dr, phantom, "\text{p.b.}"] & \in_B \arrow[d] \\ \mathcal{P}B \times A \arrow[r, "1_{\mathcal{P}B} \times f"'] & \mathcal{P}B \times B . \end{tikzcd}$$

Proof. From the definition of f^*, the corresponding relation P is given by $P = (\Gamma f \downarrow \in_B)^\circ$, so that, we have a diagram

$$\begin{tikzcd} P \arrow[r, "q_1"] \arrow[d, "q_2"'] \arrow[dr, phantom, "\leq"] & \mathcal{P}B \arrow[d, "1_{\mathcal{P}B}"] \\ A \arrow[r, "\varphi"'] & \mathcal{P}B \end{tikzcd}$$

where φ corresponds to Γf.

$$\begin{tikzcd} A \arrow[r, "\theta"'] \arrow[rr, bend left, "f"] \arrow[d, "1_A"'] \arrow[dr, phantom, "\text{p.b.}"] & \in_B \arrow[r, "q_2"'] \arrow[d, "q_1"] & B \\ A \arrow[r, "\varphi"'] & \mathcal{P}B & \end{tikzcd}$$

The property of $\Gamma f \downarrow \in_B$ given in Theorem 10 easily translates to yield the pullback

$$\begin{tikzcd} P \arrow[r, "\theta q_2"] \arrow[d, "q_2"'] \arrow[dr, phantom, "p.b."] & \in_B \arrow[d, "q_2"] \\ A \arrow[r, "f"'] & B. \end{tikzcd}$$

The pullback of the theorem now follows. $\square$

<u>Theorem 15.</u> *For all* $f: A \to B$, $x: K \to \mathcal{P}A$, $y: K \to \mathcal{P}B$ *the following property holds:*

$$y \leq \forall_f x \quad \textit{if and only if} \quad f^* y \leq x.$$

<u>Proof.</u> Let $\psi: B \to \mathcal{P}A$ correspond to $(\Gamma f)^\circ$.

$$\begin{tikzcd} P \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & A \arrow[r] \arrow[d, "f"] \arrow[rr, bend left, "1_A"] \arrow[dr, phantom, "p.b."] & \in_A \arrow[r, "q_2"'] \arrow[d, "q_1"] & A \\ Y \arrow[r, "q_2"'] & B \arrow[r, "\psi"'] & \mathcal{P}A & \end{tikzcd}$$

Let X, Y be the relations corresponding to $x: K \to \mathcal{P}A$, $y: K \to \mathcal{P}B$. Then $\forall_f x$ corresponds to the relation $((\Gamma f)^\circ \downarrow X)^\circ$ from K to B. Thus

$$y \leq \forall_f x \iff Y \leq ((\Gamma f)^\circ \downarrow X)^\circ \iff Y^\circ \leq (\Gamma f)^\circ \downarrow X$$

$\iff q_1 p_1 : P \to K$, $p_2 : P \to A$ are X-related, by Theorem 11. By Theorem 14, the monic $\begin{pmatrix} q_1 p_1 \\ p_2 \end{pmatrix} : P \rightarrowtail K \times A$ determines the relation from K to A corresponding to $f^* y$. So the result follows. $\square$

<u>Theorem 16.</u> *If* $f, g : A \to B$ *are such that* $f^* = g^* : \mathcal{P}B \to \mathcal{P}A$ *then* $f = g$. *If* f^* *is monic then* f *is epic. If* f^* *is epic then* f *is monic. If* f^* *is an isomorphism then so is* f.

<u>Proof.</u> Let $s : B \to \mathcal{P}B$ be the function corresponding to the relation $\Gamma 1_B$ from B to B. From Theorem 14 one sees that $f^* s : B \to \mathcal{P}A$ corresponds to $(\Gamma f)^\circ$ from B to A. So, if $f^* = g^*$, then $f^* s = g^* s$, so $(\Gamma f)^\circ, (\Gamma g)^\circ$ are isomorphic relations.

$$
\begin{tikzcd}
 & A \arrow[dl, "f"'] \arrow[dr, "1_A"] \arrow[dd, "h", "\cong"'] & \\
B \arrow[r, phantom, "="] & {} \arrow[r, phantom, "="] & A \\
 & A \arrow[ul, "g"] \arrow[ur, "1_A"'] &
\end{tikzcd}
$$

So $h = 1_A h = 1_A$ and $f = gh = g 1_A = g$.

Suppose f^* is monic and $uf = vf$. Then $f^* u^* = (uf)^* = (vf)^* = f^* v^*$ (using Theorem 14). So $u^* = v^*$. By above this implies $u = v$. So f is epic. A similar argument shows f^* epic implies f monic. The final sentence of the theorem now follows from Theorem 6. $\square$

<u>Theorem 17.</u> *There exists a set* 0 *with the following properties:*

(i) $\mathcal{P}0 \cong 1$;

(ii) *for all sets* A, *there exists a unique function* $0 \to A$;

(iii) *each function* $Y \to 0$ *is an isomorphism;*

(iv) *for all sets* B, $B \times 0 \cong 0$.

__Proof.__ Define $x : 1 \to \mathcal{P}(2\times 2)$ by the diagram:

$$\begin{tikzcd}
2\times 1 \arrow[r] \arrow[d, "p_2"'] \arrow[rr, bend left, "1_2\times\tau"] \arrow[dr, phantom, "\text{p.b.}"] & \in_{2\times 2} \arrow[r] \arrow[d] & 2\times 2 \\
1 \arrow[r, "x"'] & \mathcal{P}(2\times 2) &
\end{tikzcd}$$

Compose x with universal quantification along $p_1 : 2\times 2 \to 2$ to obtain a function $\forall_{p_1} x ; 1 \to \mathcal{P}2$ whose corresponding relation from 1 to 2 gives us an object O with a monic $O \to 1\times 2 \cong 2$. So $O = (((\Gamma p_1)^\circ \downarrow X)^\circ$ where X corresponds to x.

Suppose there exists $Y \to O$. Then we obtain

$$\begin{tikzcd}
 & Y \arrow[dl, "u"'] \arrow[dr, "v"] \arrow[d] & \\
1 \arrow[r, phantom, "="] & O \arrow[l] \arrow[r] & 2 \arrow[l, phantom, "="]
\end{tikzcd},$$

so $u\,(((\Gamma p_1)^\circ \downarrow X)\,v$. To apply Theorem 11, notice:

$$\begin{tikzcd}
Y\times 2 \arrow[r, "v\times 1_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "\text{p.b.}"] & 2\times 2 \arrow[r, "1_{2\times 2}"'] \arrow[d, "p_1"] & 2\times 2 \\
Y \arrow[r, "v"] \arrow[d, "u"'] & 2 & \\
1 & &
\end{tikzcd};$$

and obtain

$$\begin{tikzcd}
 & Y\times 2 \arrow[dl] \arrow[dr, "v\times 1_2"] \arrow[d, "w"] & \\
1 \arrow[r, phantom, "="] & 2\times 1 \arrow[l, "p_2"] \arrow[r, "1_2\times\tau"'] & 2\times 2 \arrow[l, phantom, "="]
\end{tikzcd}$$

from which it follows that $p_2 : Y\times 2 \to 2$ is the composite $Y\times 2 \to 1 \xrightarrow[\tau]{} 2$. Thus

$p_1 : Y\times 2 \to Y$ is an isomorphism (since the pullback of t, p_2 is Y and the pullback of t and the composite is $Y \times 2$). For any set A, to give a function $A \to \mathcal{P}Y$ is to give a relation from A to Y which is to give a monic into $A\times Y$, which is to give a function $A\times Y \to 2$, which is to give a function $f : A \times Y \to Y\times 2$ such that $p_1 f = p_2$. But p_1 is an isomorphism so there is only one such f (viz, $p_1^{-1}p_2$). So for all A there is precisely one function $A \to \mathcal{P}Y$. By Theorem 3, $\mathcal{P}Y \cong 1$.

This proves that, if there exists $Y \to 0$ then $\mathcal{P}Y \cong 1$. Since we have $1_0 : 0 \to 0$ it follows that $\mathcal{P}0 \cong 1$ which is (i). On the other hand, if we have $h : Y \to 0$ then the composite $1 \cong \mathcal{P}0 \xrightarrow{h^*} \mathcal{P}Y \cong 1$ must be 1_1, so h^* is an isomorphism. By Theorem 16, h is an isomorphism which proves (iii).

For any set A we have $A \to 1 \cong \mathcal{P}0$ which corresponds to a function $0 \to \mathcal{P}A$. Let $s : A \to \mathcal{P}A$ correspond to $\ulcorner 1_A$ and form the pullback

$$\begin{tikzcd} Z \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{p.b.}"] & A \arrow[d, "s"] \\ 0 \arrow[r] & \mathcal{P}A \end{tikzcd}$$

By (iii), $Z \to 0$ is an isomorphism so we have $0 \to Z \to A$. So we have found a function $0 \to A$. If there were two such functions their equalizer would have to be an isomorphism by (iii), and so the two would be equal. This proves (ii). By (iii), $p_2 : B \times 0 \to 0$ must be an isomorphism which proves (iv). $\square$

<u>Theorem 18.</u> <u>For all functions</u> $f : A \to B$, <u>there exist a set</u> $f(A)$, <u>a monic</u> $m : f(A) \rightarrowtail B$, <u>and an epic</u> $e : A \twoheadrightarrow f(A)$ <u>such that</u> $f = me$.

<u>Proof.</u> Let $a : 1 \to \mathcal{P}A$ correspond to the relation which is the reverse of the graph of $A \to 1$. Form the pullback

$$\begin{tikzcd}
M \arrow[r] \arrow[d, tail, "i"'] \arrow[dr, phantom, "p.b."] & 1 \arrow[d, "a"] \\
\mathcal{P}B \arrow[r, "f^*"'] & \mathcal{P}A
\end{tikzcd}$$

(so that M "consists of the subsets of B which contain the image of f"). Let $\mu : 1 \to \mathcal{P}\mathcal{P}B$ correspond to the relation M from 1 to $\mathcal{P}B$. Define $f(A)$ to be the relation from 1 to B corresponding to the composite $1 \xrightarrow{\mu} \mathcal{P}\mathcal{P}B \xrightarrow{\bigcap} \mathcal{P}B$ (see Theorem 13). More explicitly, $f(A) = M \downarrow \in_B^{\circ}$ as a relation from 1 to B. So we have a monic $m : f(A) \rightarrowtail B$.

$$\begin{tikzcd}
M \times A \arrow[r, "p_2"] \arrow[d, "1_{M\times A}"'] \arrow[dr, phantom, "p.b."] & A \arrow[r] \arrow[d, "\cong"] \arrow[dr, phantom, "p.b."] & \in_A \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & 1 \arrow[d, "\tau"] \\
M \times A \arrow[r] & 1 \times A \arrow[r, "a \times 1_A"'] & \mathcal{P}A \times A \arrow[r, "\epsilon_A"'] & 2
\end{tikzcd}$$

$$\begin{tikzcd}
M \times A \arrow[rr, dashed] \arrow[d, "1_{M\times A}"'] & \text{p.b.} & \in_B \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & 1 \arrow[d, "\tau"] \\
M \times A \arrow[r, "i \times 1_A"'] & \mathcal{P}B \times A \arrow[r, "1_{\mathcal{P}B} \times f"'] \arrow[dr, "f^* \times 1_A"'] & \mathcal{P}B \times B \arrow[r, "\epsilon_B"'] & 2 \\
 & & \mathcal{P}A \times A \arrow[ur, "\epsilon_A"'] &
\end{tikzcd}$$

Since the squares in the top diagram are pullbacks and the bottom composites of the two diagrams are equal, the dotted function exists in the bottom diagram forming a pullback. This implies that $f(X\downarrow\in_B^\circ)u$ by applying Theorem 11 to the diagram below.

$$\begin{tikzcd} M\times A \arrow[r, "p_1"] \arrow[d, "p_2"'] \arrow[dr, phantom, "p.b."] & M \arrow[r, "i"] \arrow[d] & \Omega B \\ A \arrow[r, "u"'] \arrow[d, "f"'] & 1 & \\ B & & \end{tikzcd}$$

In other words, we have:

$$\begin{tikzcd} & A \arrow[dl, "u"'] \arrow[dr, "f"] \arrow[d, "e"] & \\ 1 & X\downarrow\in_B^\circ \arrow[l] \arrow[r, tail, "m"'] & B \end{tikzcd} ,$$

and it remains to prove e is epic.

Suppose $he=ke$ and let $l: E \to f(A)$ be an equalizer of h, k. To prove $h=k$ it suffices to prove l is an isomorphism. Since $he=ke$, there exists a unique $g: A \to E$ such that $lg=e$ by the property of equalizer. Since ml is monic, the following square is a pullback.

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "1_A"'] \arrow[dr, phantom, "p.b."] & E \arrow[d, tail, "ml"] \\ A \arrow[r, "f"'] & B \end{tikzcd} .$$

Let $\xi: 1 \to \Omega B$ correspond to the relation E from

1 to B. The above pullback shows (by Theorem 14) that $f^*\xi = a$. So there exists a unique $\eta : 1 \to M$ such that $\xi = i\eta$. This means $\ulcorner\xi \leq M$ as relations from 1 to $\mathscr{P}B$. The function corresponding to $\ulcorner\xi$ is $\underline{\mathrm{sing}}_{\mathscr{P}B}\,\xi : 1 \longrightarrow \mathscr{P}\mathscr{P}B$ and that corresponding to M is μ. So $\underline{\mathrm{sing}}_{\mathscr{P}B}\,\xi \leq \mu$. By Theorem 13, $\bigcap \mu \leq \bigcap \underline{\mathrm{sing}}_{\mathscr{P}B}\,\xi = 1_{\mathscr{P}B}\,\xi = \xi$. So $f(A) \leq E$. So there exists $t : f(A) \to E$ such that $m\,l\,t = m$. So $l\,t = 1_{f(A)}$. So l is a retraction and a monic and hence (Theorem 2) an isomorphism. □

<u>Theorem 19</u>. *<u>Suppose</u>* $f : A \to B$ *<u>is a function and</u>* $s : A \to I$, $i : I \to B$ *<u>are such that</u>* $f = is$, *i <u>is monic</u>, s <u>is epic</u>. <u>Then there exists a unique isomorphism</u>* $t : f(A) \to I$ *<u>such that</u>*:

$$\begin{tikzcd}
 & f(A) \arrow[dr, "m"] \arrow[dd, "t"] & \\
A \arrow[ur, "e"] \arrow[dr, "s"'] \arrow[r, phantom, "="] & & B \arrow[l, phantom, "="] \\
 & I \arrow[ur, "i"'] &
\end{tikzcd}$$

<u>Proof</u>. Both t and its inverse can be obtained by means of Theorem 7. □

We call $f(A) \overset{m}{\rightarrowtail} B$ <u>the image of</u> f.

A <u>relation on</u> A is a relation from A to A.

An <u>equivalence relation on</u> A is a relation R on A such that, for all sets X and all functions $a, b, c : X \to A$ the following three properties hold:

<u>reflexivity</u>: $a R a$;

<u>symmetry</u>: $b R a$ implies $a R b$;

<u>transitivity</u>: $b R a$, $c R b$ imply $c R a$.

Theorem 20. *Suppose* R *is a relation on* A *and that* $r : A \to \mathcal{P}A$ *is the corresponding function (Theorem 8). The following conditions are equivalent:*

(i) R *is an equivalence relation*;

(ii) *the following square is a pullback*

$$\begin{tikzcd} R \arrow[r, "q_2"] \arrow[d, "q_1"'] \arrow[dr, phantom, "p.b."] & A \arrow[d, "r"] \\ A \arrow[r, "r"'] & \mathcal{P}A \end{tikzcd};$$

(iii) *there exists a function* $f : A \to B$ *for which the following square is a pullback*

$$\begin{tikzcd} R \arrow[r, "q_2"] \arrow[d, "q_1"'] \arrow[dr, phantom, "p.b."] & A \arrow[d, "f"] \\ A \arrow[r, "f"'] & B \end{tikzcd}.$$

Proof. (i) $\Rightarrow$ (ii). First we show $rq_1 = rq_2$. Form the pullback

$$\begin{tikzcd} P \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & R \arrow[d, "q_1"] \\ R \arrow[r, "q_1"'] & A \end{tikzcd}.$$

Then $q_2p_1 R q_1p_1$, $q_2p_2 R q_1p_2$, $q_1p_1 = q_1p_2$ and symmetry-transitivity imply $q_2p_2 R q_2p_1$. So there exists $p : P \to R$ such that $q_1p = q_2p_1$, $q_2p = q_2p_2$. The pullback property of P together with symmetry-transitivity of R show that the following square is a pullback.

$$\begin{tikzcd} P \arrow[r, "p"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & R \arrow[d, "q_1"] \\ R \arrow[r, "q_2"'] & A \end{tikzcd}$$

It follows that the relation P from R to A corresponds to both rq_1 and rq_2. So $rq_1 = rq_2$.

Suppose $a, b : X \to A$ are such that $ra = rb$.

$$\begin{tikzcd} Q \arrow[r, shift left, "u"] \arrow[r, shift right, "v"'] \arrow[d, "w"'] & R \arrow[r] \arrow[rr, bend left, "q_2"] \arrow[d, "q_1"] \arrow[dr, phantom, "p.b."] & \in_A \arrow[r] \arrow[d] & A \\ X \arrow[r, shift left, "a"] \arrow[r, shift right, "b"'] & A \arrow[r, "r"'] & PA & \end{tikzcd}$$

Then, in the above diagram, $q_2 u = q_2 v$, the set Q together with w, u are a pullback of a, q_1, and Q together with w, v are a pullback of b, q_1. By reflexivity, $1_A R 1_A$. So there exists $x : A \to R$ such that $q_1 x = 1_A = q_2 x$. Now $q_1 x b = b 1_X$ implies there exists $y : X \to Q$ such that $wy = 1_X$ and $vy = xb$ (using pullback property of Q). Then $q_1 u y = a w y = a 1_X = a$, $q_2 u y = q_2 v y = q_2 x b = 1_A b = b$. Finally, uy is unique such that $q_1 u y = a$, $q_2 u y = b$ since $\binom{q_1}{q_2}$ is monic.

(ii) $\Rightarrow$ (iii). By (ii), r is such an f.

(iii) $\Rightarrow$ (i) The pullback property can be stated in the form: for all $a, b : X \to A$, bRa if and only if $fa = fb$. The properties of an equivalence relation are obvious from this. $\square$

Suppose R is a relation from A to B and S is a relation from B to C. Form the pullback

$$\begin{tikzcd} P \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & S \arrow[d, "q_1"] \\ R \arrow[r, "q_2"'] & B, \end{tikzcd}$$

and factor the composite $P \xrightarrow{\binom{p_1}{p_2}} R \times S \xrightarrow{q_1 \times q_2} A \times C$ into an epic and monic $P \twoheadrightarrow SR \rightarrowtail A \times C$ using Theorem 18. The relation SR from A to C is called <u>the composite of</u> R <u>and</u> S.

<u>Theorem 21</u>. $SR \leq T$ <u>if and only if</u> $R \leq S \downarrow T$.

<u>Proof</u>. By Theorem 11, $R \leq S \downarrow T$ if and only if $q_2 p_2 \, T \, q_1 p_1$. This happens when there is a function $P \longrightarrow T$ such that the two composites in the diagram

$$\begin{tikzcd} P \arrow[r, two heads] \arrow[d] & SR \arrow[d, tail] \\ T \arrow[r, tail] & A \times C \end{tikzcd}$$

are equal. By Theorem 7 this happens when $SR \leq T$. $\square$

We can now define existential quantification in the same spirit as universal quantification was defined earlier.

<u>Existential quantification along a relation</u> R from A to B is the function $\exists_R : \mathcal{P}A \longrightarrow \mathcal{P}B$ corresponding to the relation $R \in_A$ from $\mathcal{P}A$ to B. For $f : A \to B$, write $\exists_f$ for $\exists_{\ulcorner f}: \mathcal{P}A \to \mathcal{P}B$. The intuitive formula for $\exists_R$ is:

$\exists_R X = \{ b \in B \mid \text{there exists } a \in X \text{ such that } bRa \}$.

The set $\mathcal{P}(A\times B)$ can be thought of as <u>the set of relations from</u> A <u>to</u> B. We now wish to cut down this set to give the set $\mathcal{P}ar(A,B)$ of <u>partial functions</u> (or "functions which are not necessarily everywhere defined") <u>from</u> A <u>to</u> B. Form the pullback:

$$\begin{tikzcd}
M \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "p.b."] & \in_{A\times B} \arrow[r, "p_2 q_2"] \arrow[d, "\binom{q_1}{p_1 q_2}"] & B \\
\in_{A\times B} \arrow[r, "\binom{q_1}{p_1 q_2}"'] \arrow[d, "p_2 q_2"'] & \mathcal{P}(A\times B)\times A & \\
B & &
\end{tikzcd}$$

This gives a relation M from $\mathcal{P}(A\times B)$ to $A\times B\times B$ (intuitively given by $\begin{pmatrix} a \\ b \\ b' \end{pmatrix} M S$ when bSa and $b'Sa$); let $\mu : \mathcal{P}(A\times B) \to \mathcal{P}(A\times B\times B)$ denote the corresponding function. There is also the relation

$$\in_{A\times B} \rightarrowtail \mathcal{P}(A\times B)\times A\times B \xrightarrow[1\times\binom{1}{1}]{} \mathcal{P}(A\times B)\times A\times B\times B$$

from $\mathcal{P}(A\times B)$ to $A\times B\times B$ which corresponds to a function $\delta : \mathcal{P}(A\times B) \to \mathcal{P}(A\times B\times B)$. Define $\mathcal{P}ar(A,B)$ to be an equalizer of μ, δ:

$$\mathcal{P}ar(A,B) \rightarrowtail \mathcal{P}(A\times B) \underset{\delta}{\overset{\mu}{\rightrightarrows}} \mathcal{P}(A\times B\times B).$$

Intuitively, S is a partial function means bSa and $b'Sa$ only when $b=b'$; the universal formulation of this is the next theorem.

<u>Theorem 22. *Let* S *denote the relation from* C *to* $A \times B$ *corresponding to a function* $s : C \to \mathcal{P}(A \times B)$. *The function*</u>

$$\begin{pmatrix} q_1 \\ p_1 q_2 \end{pmatrix} : S \longrightarrow C \times A$$

<u>*is monic if and only if* s *factors through*</u>
$Par(A,B) \rightarrowtail \mathcal{P}(A \times B)$.

<u>Proof</u>. The relation P corresponding to μs is given by:

$$\begin{tikzcd}
P \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & S \arrow[r, "p_2 q_2"] \arrow[d, "\begin{pmatrix} q_1 \\ p_1 q_2 \end{pmatrix}"] & B \\
S \arrow[r, "\begin{pmatrix} q_1 \\ p_1 q_2 \end{pmatrix}"'] \arrow[d, "p_2 q_2"'] & C \times A & \\
B & &
\end{tikzcd}$$

The relation corresponding to δs is just:

$$S \rightarrowtail C \times A \times B \xrightarrow{1 \times \binom{1}{1}} C \times A \times B \times B.$$

Now s factors as required if and only if $\mu s = \delta s$; so this happens when the square

$$\begin{tikzcd}
S \arrow[r, "1"] \arrow[d, "1"'] & S \arrow[d] \\
S \arrow[r] & C \times A
\end{tikzcd}$$

is a pullback, which just says $S \to C \times A$ is monic. □

In particular we can apply this theorem when s is the monic $Par(A,B) \rightarrowtail \mathcal{P}(A \times B)$. This gives a monic $Dom \rightarrowtail Par(A,B) \times A$ which can be regarded as a relation from $Par(A,B)$ to A. The corresponding function is denoted by:

$$\underline{dom} : Par(A,B) \longrightarrow \mathcal{P}A.$$

Suppose T is a relation from A to C. For $u : X \to C$, write $T(u)$ for the pullback of $q_2 : T \to C$ and $u : X \to C$. Suppose $u = vf$ in the triangle below.

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "u"'] & & Y \arrow[dl, "v"] \\ & C & \end{tikzcd}$$

There is a function $Tf : T(u) \to T(v)$ induced satisfying $p_1(Tf) = p_1$, $p_2(Tf) = f p_2$.

<u>Theorem 23</u>. *For each relation* T *from* A *to* C *and each set* B, *there exist functions*

$$p_B : T \pitchfork B \to C, \qquad \varepsilon^T_B : T(p_B) \to B$$

with the following property: for all functions

$$u : X \to C, \qquad v : T(u) \to B,$$

there exists a unique function $f : X \to T \pitchfork B$ *such that* $pf = u$ *and* $\varepsilon^T_B(Tf) = v$.

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "u"'] & & T \pitchfork B \arrow[dl, "p"] \\ & C & \end{tikzcd} \qquad \begin{tikzcd} T(u) \arrow[rr, "Tf"] \arrow[dr, "v"'] & & T(p) \arrow[dl, "\varepsilon^T_B"] \\ & B & \end{tikzcd}$$

<u>Proof.</u> Let $t^\circ : C \to \wp A$ be the function corresponding to T° and form the pullback

$$\begin{tikzcd} T \pitchfork B \arrow[r, "p_2"] \arrow[d, "p_B"'] \arrow[dr, phantom, "p.b."] & \wp ar(A,B) \arrow[d, "\underline{dom}"] \\ C \arrow[r, "t^\circ"'] & \wp A . \end{tikzcd}$$

We now examine what it is to give a diagram:

$$\begin{tikzcd} X \arrow[r, "w"] \arrow[d, "u"'] & \mathcal{P}ar(A,B) \arrow[d, "\underline{dom}"] \\ C \arrow[r, "t^0"'] & \mathcal{P}A \end{tikzcd}$$

in which $\underline{dom}\, w = t^0 u$. To give w is to give $s : X \longrightarrow \mathcal{P}(A\times B)$ such that the corresponding S has $S \longrightarrow C\times A$ monic (Theorem 22). The relation from X to A corresponding to $t^0 u$ is precisely $\begin{pmatrix} p_2 \\ q_1 p_1 \end{pmatrix} : T(u) \rightarrowtail X\times A$. So the condition $t^0 u = \underline{dom}\, w$ gives the diagram:

$$\begin{tikzcd} T(u) \arrow[r] \arrow[d, "\begin{pmatrix} p_2 \\ q_1p_1 \\ v \end{pmatrix}"'] \arrow[dd, bend right=60, "\begin{pmatrix} p_2 \\ q_1p_1 \end{pmatrix}"'] \arrow[dr, phantom, "p.b."] & \mathrm{Dom} \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & \in_{A\times B} \arrow[d] \\ X\times A\times B \arrow[r, "w\times 1"'] \arrow[d, "1\times p_1"'] \arrow[dr, phantom, "p.b."] & \mathcal{P}ar(A,B)\times A\times B \arrow[r, "i\times 1"] \arrow[d, "1\times p_1"'] \arrow[dr, phantom, "p.b."] & \mathcal{P}(A\times B)\times A\times B \arrow[d, "1\times p_1"] \\ X\times A \arrow[r, "w\times 1"'] & \mathcal{P}ar(A,B)\times A \arrow[r, "i\times 1"'] & \mathcal{P}(A\times B)\times A \end{tikzcd}$$

So we obtain a function $v : T(u) \longrightarrow B$. Conversely, given $v : T(u) \longrightarrow B$ we obtain a relation $\begin{pmatrix} p_2 \\ q_1p_1 \\ v \end{pmatrix} : T(u) \rightarrowtail X\times A\times B$ from X to $A\times B$ for which $T(u) \longrightarrow X\times A$ is monic; by Theorem 22, we recover $w : X \longrightarrow \mathcal{P}ar(A,B)$ with $\underline{dom}\, w = t^0 u$. In other words, to give w such that $\underline{dom}\, w = t^0 u$ is precisely to give $v : T(u) \longrightarrow B$.

In particular, taking $u = p_B$, $w = p_2$, $X = T \pitchfork B$, we obtain $\varepsilon_B^T : T(p) \longrightarrow B$.

Suppose $u : X \longrightarrow C$, $v : T(u) \longrightarrow B$ are functions and let $w : X \longrightarrow \mathcal{P}ar(A,B)$ correspond to v as above. Since $\underline{\mathrm{dom}}\, w = t^{\circ}u$, there exists a unique $f: X \longrightarrow T \pitchfork B$ such that $p_B f = u$ and $p_2 f = w$. It is left to the reader to check that the condition $p_2 f = w$ amounts precisely to $\varepsilon_B^T(Tf) = v$. $\square$

__Theorem 24.__ *If $u: X \longrightarrow C$ is epic and the square*

$$\begin{tikzcd} P \arrow[r, "p_2"] \arrow[d, "p_1"'] & X \arrow[d, "u"] \\ A \arrow[r, "g"'] & C \end{tikzcd}$$

is a pullback then p_1 is an epic.

__Proof.__ Let T denote the graph of g from A to C. We have a triangle

$$\begin{tikzcd} X \arrow[rr, "u"] \arrow[dr, "u"'] & & C \arrow[dl, "1_C"] \\ & C & \end{tikzcd},$$

and $Tu: T(u) \longrightarrow T(1_C)$ is just $p_1: P \longrightarrow A$. Suppose $h, k: A \longrightarrow Y$ are such that $hp_1 = kp_1$.

$$\begin{tikzcd} T(u) \arrow[r, "Tu"] & T(1_C) \arrow[r, shift left, "h"] \arrow[r, shift right, "k"'] & Y \end{tikzcd}$$

By Theorem 23, there exist unique $h', k': C \longrightarrow T \pitchfork Y$ such that $p_Y h' = p_Y k' = 1_C$, $\varepsilon_Y^T(Th') = h$, $\varepsilon_Y^T(Tk') = k$. From $h(Tu) = k(Tu)$ it follows that (Theorem 23) $h'u = k'u$. Since u is epic, $h' = k'$. But then $h = \varepsilon_Y^T(Th') = \varepsilon_Y^T(Tk') = k$. So p_1 is epic. $\square$

Recall from the exercises that it is a much more trivial fact that the same result holds with "epic" replaced by "monic".

<u>Theorem 25.</u> *Suppose* R *is a relation from* A *to* B, S *is a relation from* B *to* C, *and* T *is a relation from* C *to* D, *then there is an isomorphism*

$$(TS)R \cong T(SR)$$

of relations from A *to* D.

<u>Proof.</u> Form the pullbacks:

$$\begin{tikzcd}
 & & & P_3 \arrow[dl] \arrow[dr] \arrow[dd, phantom, "p.b."] & & & \\
 & & P_1 \arrow[dl] \arrow[dr] \arrow[dd, phantom, "p.b."] & & P_2 \arrow[dl] \arrow[dr] \arrow[dd, phantom, "p.b."] & & \\
 & R \arrow[dl] \arrow[dr] & & S \arrow[dl] \arrow[dr] & & T \arrow[dl] \arrow[dr] & \\
A & & B & & C & & D
\end{tikzcd}$$

It follows that the pullback of $P_1 \longrightarrow A \times C$ and $A \times T \longrightarrow A \times C$ is P_3; so we have:

$$\begin{tikzcd}
P_3 \arrow[r, two heads] \arrow[d] \arrow[dr, phantom, "pb"] & Q_1 \arrow[r, tail] \arrow[d] \arrow[dr, phantom, "pb"] & A \times T \arrow[d] \\
P_1 \arrow[r, two heads] & SR \arrow[r, tail] & A \times C,
\end{tikzcd}$$

where $P_3 \longrightarrow Q_1$ is epic by Theorem 24. Now $T(SR)$ is the image of $Q_1 \rightarrowtail A \times T \longrightarrow A \times D$; so we have $P_3 \twoheadrightarrow Q_1 \twoheadrightarrow T(SR) \rightarrowtail A \times D$. By Theorem 19, $T(SR)$ is (up to isomorphism) the image of $P_3 \longrightarrow A \times D$. By symmetry, $(TS)R$ is also isomorphic to the image of $P_3 \longrightarrow A \times D$. $\square$

This allows us to prove a powerful relationship between existential and universal quantification which is valid even for the intuitionist. It generalizes Theorem 15.

<u>Theorem 26.</u> *For any relation R from A to B,*

$$1_{\wp A} \leq \forall_{R^\circ} \exists_R \quad \text{and} \quad \exists_R \forall_{R^\circ} \leq 1_{\wp B}.$$

<u>Proof.</u> $\forall_{R^\circ}$, $\exists_R$ correspond to the relations $(R\downarrow \in_B)^\circ$, $R\in_A$. It follows from Theorem 10 that $\forall_{R^\circ}\exists_R$ corresponds to $R\downarrow R\in_A$. By Theorem 21, $R\in_A \leq R\in_A$ implies $\in_A \leq R\downarrow R\in_A$ which gives the first inequality.

One easily sees that $\exists_R \forall_{R^\circ}$ corresponds to the relation $(R\in_A)(\Gamma\forall_{R^\circ})$ which is isomorphic to $R(\in_A(\Gamma\forall_{R^\circ}))$ by the last theorem. But $\in_A(\Gamma\forall_{R^\circ}) \cong R\downarrow\in_B$ by definition of $\forall_{R^\circ}$. So $\exists_R\forall_{R^\circ}$ corresponds to $R(R\downarrow\in_B)$. By Theorem 21, $R\downarrow\in_B \leq R\downarrow\in_B$ implies $R(R\downarrow\in_B)\leq\in_B$ which gives the second inequality. $\square$

<u>Theorem 27.</u> *If R is a relation from A to B and S is a relation from B to C then*

$$\exists_{SR} = \exists_S\exists_R \quad \text{and} \quad \forall_{SR} = \forall_S \forall_R.$$

<u>Proof.</u> From Theorem 10 and the following diagram

$$\begin{tikzcd}
S^\circ\downarrow(R^\circ\downarrow\in_A) \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & R^\circ\downarrow\in_A \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & \wp A \arrow[d, "\forall_R"] \\
S^\circ\downarrow\in_B \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & \in_B \arrow[r] \arrow[d] \arrow[dr, phantom, "\leqslant"] & \wp B \arrow[d, "1"] \\
C \arrow[r, "s^\circ"'] & \wp B \arrow[r, "1"'] & \wp B
\end{tikzcd}$$

we see that $\forall_S\forall_R$ corresponds to $(S^\circ\downarrow(R^\circ\downarrow\in_A))^\circ$.

But $U \leq S^\circ \downarrow (R^\circ \downarrow \in_A) \overset{\text{Thm 21}}{\Longleftrightarrow} S^\circ U \leq R^\circ \downarrow \in_A \overset{\text{Thm 21}}{\Longleftrightarrow} R^\circ(S^\circ U) \leq \in_A \overset{\text{Thm 25}}{\Longleftrightarrow} (SR)^\circ U \leq \in_A \overset{\text{Thm 21}}{\Longleftrightarrow} U \leq (SR)^\circ \downarrow \in_A$. The fact that this holds for all relations U from B to $\mathcal{P}A$ implies $S^\circ \downarrow (R^\circ \downarrow \in_A) \cong (SR)^\circ \downarrow \in_A$. It follows that $\forall_S \forall_R \cong \forall_{SR}$.

It follows easily from Theorem 26 that $\exists_R x \leq y$ if and only if $x \leq \forall_{R^\circ} y$. So $\exists_S \exists_R \leq z \Longleftrightarrow \exists_R \leq \forall_{S^\circ} z \Longleftrightarrow 1_{\mathcal{P}A} \leq \forall_{R^\circ} \forall_{S^\circ} z = \forall_{(SR)^\circ} z \Longleftrightarrow \exists_{SR} \leq z$. Since this holds for all z, $\exists_S \exists_R = \exists_{SR}$. $\Box$

<u>Theorem 28</u>. <u>Suppose</u> $f: A \to B$, $g: B \to C$ <u>are epic and that both the ~~second square~~ square below is a pullback</u>

$$\begin{tikzcd} P \arrow[r, "v"] \arrow[d, "u"'] & A \arrow[d, "f"] \\ A \arrow[r, "f"'] & B \end{tikzcd} \qquad \begin{tikzcd} P \arrow[r, "v"] \arrow[d, "u"'] \arrow[dr, phantom, "\text{p.b.}"] & A \arrow[d, "gf"] \\ A \arrow[r, "gf"'] & C \end{tikzcd}$$

<u>and ~~$fu = fv$~~. Then</u> g <u>is an isomorphism</u>.

<u>Proof</u>. We have the following diagram of pullbacks:

$$\begin{tikzcd} P \arrow[r] \arrow[d] \arrow[rr, bend left, "v"] \arrow[dd, bend right, "u"'] \arrow[dr, phantom, "\text{p.b.}"] & M \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{p.b.}"] & A \arrow[d, "f"] \\ N \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{p.b.}"] & Q \arrow[r, "s"] \arrow[d, "r"] \arrow[dr, phantom, "\text{p.b.}"] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & B \arrow[r, "g"'] & C \end{tikzcd}$$

Since f is epic, it follows from Theorem 24 that $e: P \to Q$ is epic. Since $fu = fv$ it follows that $re = se$. So $r = s$. So g is monic. Theorem 6 now gives the result. $\square$

Theorem 29. Suppose $e : A \to B$ is epic and the square

$$\begin{array}{ccc} R & \xrightarrow{q_2} & A \\ {\scriptstyle q_1}\downarrow & & \downarrow{\scriptstyle e} \\ A & \xrightarrow[e]{} & B \end{array}$$

is a pullback. For all functions $h : A \to Y$ such that $hq_1 = hq_2$, there exists a unique function $k : B \to Y$ such that $ke = h$.

Proof. With h as given, factor $\binom{e}{h} : A \to B \times Y$ into an epic and monic

$$\begin{tikzcd} A \arrow[rr, "\binom{e}{h}"] \arrow[dr, "f"'] & & B \times Y \\ & I \arrow[ur, "m"'] & \end{tikzcd}.$$

Put $g = p_1 m : I \to B$ and note that $gf = p_1 m f = p_1\binom{e}{h} = e$. So q_1, q_2 are a pullback of gf, gf. Also $mfq_1 = \binom{e}{h}q_1 = \binom{eq_1}{hq_1} = \binom{eq_2}{hq_2} = \binom{e}{h}q_2 = mfq_2$ and m is monic. So $fq_1 = fq_2$. By Theorem 28, g is an isomorphism. Take k to be the composite:

$$B \xrightarrow{g^{-1}} I \xrightarrow{m} B \times Y \xrightarrow{p_2} Y.$$

So $ke = p_2 m g^{-1} e = p_2 m f = p_2\binom{e}{h} = h$ (since $f = g^{-1}\eta$). The uniqueness of k follows from the fact that e is epic. $\square$

Suppose R is an equivalence relation on A, and let $r : A \to \mathcal{P}A$ be the corresponding function (Theorem 8). The image $r(A)$ of r is called <u>the set of equivalence classes of</u> R and denoted by A/R; so we have:

$$\begin{tikzcd} A \arrow[rr, "r"] \arrow[dr, "\eta"'] & & \mathcal{P}A \\ & A/R \arrow[ur, "\mu"'] & \end{tikzcd}.$$

The function η is called <u>the canonical epic</u>.
Since μ is monic, Theorem 20 yields a pullback:

$$\begin{tikzcd} R \arrow[r, "q_2"] \arrow[d, "q_1"'] \arrow[dr, phantom, "p.b."] & A \arrow[d, "\eta"] \\ A \arrow[r, "\eta"'] & A/R \end{tikzcd}.$$

Theorem 29 now applies: to give a function $k : A/R \to Y$ with domain A/R is precisely to give a function $h : A \to Y$ such that $hq_1 = hq_2$ (that is, h "identifies R-related things").

The next result is called <u>the first isomorphism theorem</u>.

<u>Theorem 30</u>. <u>If the following square is a pullback</u>

$$\begin{tikzcd} R \arrow[r, "q_2"] \arrow[d, "q_1"'] \arrow[dr, phantom, "pb"] & A \arrow[d, "f"] \\ A \arrow[r, "f"'] & B \end{tikzcd}$$

<u>then there is an isomorphism</u> $\varphi : A/R \cong f(A)$ <u>which composes with the canonical epic</u> $\eta : A \to A/R$ <u>and the "inclusion"</u> $m : f(A) \rightarrowtail B$ <u>to yield</u> f.

<u>Proof</u>. In the notation of Theorem 18, since m is monic, the pullback above gives the pullback

$$\begin{tikzcd} R \arrow[r, "q_2"] \arrow[d, "q_1"'] & A \arrow[d, "e"] \\ A \arrow[r, "e"'] & f(A). \end{tikzcd}$$

By Theorem 29, e is the universal function out of A which makes q_1, q_2 equal. But $\eta : A \to A/R$ is too. These universal properties give an isomorphism φ such that $\varphi\eta = e$. So $m\varphi\eta = me = f$ as required. $\square$

Recall the fundamental rôle played by $\cap : \wp B \times \wp B \longrightarrow \wp B$ (see Theorem 9). For $r, s : A \to \wp B \times \wp B$, we define $r \leq s$ when $p_1 r \leq p_1 s$ and $p_2 r \leq p_2 s$. It follows easily from Theorem 9 that

$$1_{\wp B} = \cap\,\delta \quad \text{and} \quad \delta\cap \leq 1_{\wp B \times \wp B},$$

where $\delta : \wp B \longrightarrow \wp B \times \wp B$ is defined by $p_1\delta = p_2\delta = 1_{\wp B}$.

<u>Theorem 31.</u> *The function* $\cup : \wp B \times \wp B \longrightarrow \wp B$ *obtained as the composite*

$$\wp B \times \wp B \xrightarrow{\underline{up} \times \underline{up}} \wp\wp B \times \wp\wp B \xrightarrow{\ \cap\ } \wp\wp B \xrightarrow{\ \bigcap\ } \wp B$$

has the following properties:

$$\cup\,\delta = 1_{\wp B} \quad \text{and} \quad 1_{\wp B \times \wp B} \leq \delta\,\cup .$$

<u>Proof.</u> Theorem 9 easily yields $\cap(\underline{up} \times \underline{up}) \leq \underline{up}\, p_i$ for $i = 1, 2$. So, by Theorem 13, $p_i \leq \bigcap \cap (\underline{up} \times \underline{up}) = \cup$. So $1 \leq \delta\cup$. On the other hand, $\cup\,\delta = \bigcap \cap \binom{\underline{up}}{\underline{up}} = \bigcap \underline{up} = 1$ using the same two theorems. $\square$

Theorem 32. *For relations* R, R' *from* A *to* B, *there is a relation* $R \cup R'$ *from* A *to* B *such that* $R \leq R \cup R'$, $R' \leq R \cup R'$, *and, if* $R \leq S$, $R' \leq S$ *then* $R \cup R' \leq S$. *Furthermore, for all* $u : Y \to B$, $(R \cup R')(u) \cong R(u) \cup R'(u)$ *as relations from* A *to* Y.

Proof. Define $R \cup R'$ to correspond to $\cup\binom{\rho}{\rho'}$ where R, R' correspond to $\rho, \rho' : 1 \to \mathcal{P}(A \times B)$. The first sentence follows from Theorem 31 and the second from Theorem 15. $\square$

Theorem 33. *For all sets* A, B, *there exist a set* $A+B$ *and functions* $i_1 : A \to A+B$, $i_2 : B \to A+B$ *with the following property: for all* $h : A \to Y$, $k : B \to Y$, *there exists a unique* $l : A+B \to Y$ *such that* $h = l i_1$, $k = l i_2$. *Moreover,* $\mathcal{P}(A+B)$ *together with* i_1^*, i_2^* *is a product for* $\mathcal{P}A$, $\mathcal{P}B$, *and the following square is a pullback*

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & B \arrow[d, "i_2"] \\
A \arrow[r, "i_1"'] & A+B
\end{tikzcd}$$

Proof. Let $m_A : A \to \mathcal{P}A \times \mathcal{P}B$ denote the function for which $p_1 m_A = \underline{\text{sing}}_A$ and $p_2 m_A$ is the composite $A \to 1 \xrightarrow{0} \mathcal{P}B$ (where 0 is the subset of B corresponding to the monic $0 \rightarrowtail B$). Now m_A is monic since $\underline{\text{sing}}_A$ is, and we write $\bar{A}$ for the corresponding relation from 1 to $\mathcal{P}A \times \mathcal{P}B$. Symmetrically we obtain $\bar{B}$ from 1 to $\mathcal{P}A \times \mathcal{P}B$. Put $A+B = \bar{A} \cup \bar{B}$; so we have a diagram:

$$\begin{tikzcd}
 & A \arrow[dl] \arrow[d, "i_1"] \arrow[dr, "m_A"] & \\
1 & A+B \arrow[l] \arrow[r, tail, "j"] & \mathcal{P}A\times\mathcal{P}B \\
 & B \arrow[ul] \arrow[u, "i_2"'] \arrow[ur, "m_B"'] &
\end{tikzcd}$$

By pullback along $C \longrightarrow 1$ we obtain a diagram

$$\begin{tikzcd}
 & C\times A \arrow[dl, "p_1"'] \arrow[d, "1\times i_1"] \arrow[dr, "m_A p_2"] & \\
C & C\times(A+B) \arrow[l, "p_1"'] \arrow[r, "j p_2"] & \mathcal{P}A\times\mathcal{P}B \\
 & C\times B \arrow[ul, "p_1"] \arrow[u, "1\times i_2"'] \arrow[ur, "m_B p_2"'] &
\end{tikzcd}$$

in which $C\times(A+B) \cong (C\times A)\cup(C\times B)$ as relations from C to $\mathcal{P}A\times\mathcal{P}B$ (Theorem 32).

Each relation T from C to $A+B$ yields relations $T(i_1)$, $T(i_2)$ from C to A, B, respectively.

Conversely, relations T_1, T_2 from C to A, B can be regarded as relations from C to $\mathcal{P}A\times\mathcal{P}B$ for which $T_1 \leq C\times A$, $T_2 \leq C\times B$. Then $T_1\cup T_2 \leq C\times(A+B)$ (Theorem 32), so $T_1\cup T_2$ is a relation from C to $A+B$.

Suppose the following square commutes.

$$\begin{tikzcd}
X \arrow[r, "v"] \arrow[d, "u"'] & B \arrow[d, "i_2"] \\
A \arrow[r, "i_1"'] & A+B
\end{tikzcd}$$

Then $m_A u = m_B v$. So $p_1 m_A u = p_2 m_B v$. So $\Gamma u \cong 0$ as relations from X to A. So $X \cong 0$.

So the pullback of i_1, i_2 is 0.

It follows now by Theorem 32 that $(T_1 \cup T_2)(i_1) \cong T_1(i_1) \cup T_2(i_1) \cong T_1 \cup 0 \cong T_1$ and $(T_1 \cup T_2)(i_2) \cong T_2$.

Also $T(i_1) \leq T$, $T(i_2) \leq T$. Suppose S is such that $T(i_1) \leq S$, $T(i_2) \leq S$ as relations from C to $\mathcal{P}A \times \mathcal{P}B$. Write T', $\bar{S}$ for the relations

$$\mathcal{P}A \times \mathcal{P}B \xleftarrow{q_2} T \xrightarrow{\binom{q_1}{q_2}} C \times \mathcal{P}A \times \mathcal{P}B$$

$$1 \longleftarrow S \xrightarrow{\binom{q_1}{q_2}} C \times \mathcal{P}A \times \mathcal{P}B$$

from $\mathcal{P}A \times \mathcal{P}B$ to $C \times \mathcal{P}A \times \mathcal{P}B$, and from 1 to $C \times \mathcal{P}A \times \mathcal{P}B$, respectively. Notice that $T(i_1) = T'\bar{A}$, $T(i_2) = T'\bar{B}$. By Theorem 21, $\bar{A} \leq T' \downarrow \bar{S}$, $\bar{B} \leq T' \downarrow \bar{S}$. By Theorem 32, $A+B = \bar{A} \cup \bar{B} \leq T' \downarrow \bar{S}$. By Theorem 21, $T'(A+B) \leq \bar{S}$. Since $T \leq C \times (A+B)$, the relation $T'(A+B)$ is just $\bar{T}$. So $\bar{T} \leq \bar{S}$ which amounts to $T \leq S$. So $T \cong T(i_1) \cup T(i_2)$.

So, to give a relation T from C to $A+B$ (up to isomorphism) is to give relations T_1, T_2 from C to A, B (up to isomorphism). By Theorem 8, this is to give a function $t : C \longrightarrow \mathcal{P}A \times \mathcal{P}B$. Using Theorem 8, we can now deduce an isomorphism

$$\mathcal{P}A \times \mathcal{P}B \cong \mathcal{P}(A+B).$$

Suppose $h : A \to Y$, $k : B \to Y$, and let T be the relation from Y to $A+B$ such that $T(i_1) \cong (\Gamma h)^\circ$, $T(i_2) \cong (\Gamma k)^\circ$. Then $T(i_1) \leq Y \times A$ and $T(i_2) \leq Y \times B$, so $T = T(i_1) \cup T(i_2) \leq Y \times (A+B)$ and relations from Y to $\mathcal{P}A \times \mathcal{P}B$. It follows that $q_2 : T \longrightarrow A+B$ is an isomorphism. This gives $l = q_1 q_2^{-1} : A+B \longrightarrow Y$ as required. Uniqueness is easily checked. $\square$