Math 365: Really Basic Stuff

The *product* of two sets A and B is the set

$$A \times B\{(a, b) : a \in A, b \in B\}$$

comprising all ordered pairs of elements from A and B, respectively. Any $R \subset A \times B$ is called a $r$elation between A and B.

Note that a relation is nothing more than a list of ordered pairs. In practice, there are often 'rules' explaining which pairs are in and which are out, but in principle no such rule need exist beyond the list itself.

Let $R \subset A \times B$ and $S \subset B \times C$ be relations. The *inverse* of R is the relation

$$R^{-1}\{(b, a) \in B \times A : (a, b) \in R\}.$$

The composition of S and R is the relation

$$S \circ R\{(a, c) \in A \times C : \text{ there is } b \in B \text{ such that } (a, b) \in R \text{ and } (b, c) \in S\}.$$

The *identity* (or *diagonal*) relation on a set A is

$$id = \{(a, a) : a \in A\}$$

Let A be the set of people and B the set of all kinds of food. The set

$$R = \{(a, b) \in A \times B : a \text{ likes to eat } b\}$$

is a relation. It's inverse is just obtained by switching first and second entries in each ordered pair. The composition of R^{-1} with R is

$$R^{-1} \circ R = \{(x, y) \in A : x \text{ and } y \text{ have some food in common that both like to eat}\}.$$

Most of our relations will concern sets of numbers. For example,

$$\{(x, y) \in : y = x^2\}.$$

A relation $R \subset A \times B$ is called a *function with domain* A if for each $a \in A$, there is a unique element $b \in B$ such that $(a, b) \in R$.

So the last example was a function with domain . Of course, notationally, we will always write $R : A \to B$ and $b = R(a)$, rather than $R \subset A \times B$ and $(a, b) \in R$. The following statement is intuitively obvious and its proof is practically void of content, but it does show how one manipulates the ordered pair definition of 'function' in order to achieve a modest goal.

Given functions $R \subset A \times B$ and $S \subset B \times C$ with domains A and B respectively, $S \circ R$ is a function with domain A.

By definition $S \circ R$ is a relation between A and C. Let $a \in A$ be any given element. Since A is the domain of R and B the domain of S, there are elements $b \in B, c \in C$ such that $(a, b) \in R$ and $(b, c) \in S$. So $(a, c) \in S \circ R$. That is, given $a \in A$ there exists $c \in C$ such that $(a, c) \in S \circ R$.

To establish uniqueness of c, suppose also that $(a, c') \in S \circ R$. Then there is $b' \in B$ such that $(a, b') \in R$, $(b', c') \in S$. Since R and S are functions, it follows that $b' = b$ and therefore that $c' = c$, as well. Hence c is unique, and $S \circ R$ is a function.

One kind of function that is particularly common arises every time you multiply or add two numbers together.

A binary operation on a set A is a function $* : A \times A \to A$ (who says one has to use a letter to denote something?).

Again, convention means a great deal, and one never really writes $((x, y), z) \in *$ or even $*(x, y) = z$ when one is dealing with a binary operation. Rather, one writes $x * y = z$ (unless one uses reverse Polish notation, which is another story entirely...). So that's the plain truth folks. The addition you learned in the first grade—$1 + 1 = 2, 2 + 1 = 3$—and all that, is really just a subset of the product set $(\times)\times$ that includes the elements $((1, 1), 2), ((1, 2), 3)$ among others. Bet you felt like there was something missing in your lives up til now...

Functions aren't the only type of relation that one typically sees.

An *equivalence relation* on A is a relation $\sim \subset A \times A$ with the following three properties. For every $a, b, c \in A$.

- (reflexivity) $(a, a) \in \sim$.
- (symmetry) $(a, b) \in \sim$ implies $(b, a) \in \sim$.
- (transitivity) $(a, b) \in \sim, (b, c) \in \sim$ implies $(a, c) \in \sim$.

When it's an equivalence relation we're talking about, tradition dictates that we write $a \sim b$ instead of $(a, b) \in \sim$. The archetypal equivalence relation is the identity relation id (a.k.a. '=') described earlier. Note that this one has the peculiar property of being both an equivalence relation and a function simultaneously! Are there any other such relations you can think of?

Here's are a couple of other examples of equivalence relations. Where do you suppose we get the second one?

Let A be the set of people and say $a \sim b$ if a and b have the same first name. This is an equivalence relation.

The relation on $\times^+$ given by $(p, q) \sim (r, s)$ if and only if $ps = rq$ is an equivalence relation.

You write it.

Equivalence relations are great for dividing the world into 'us' and various kinds of 'them'.

Given an equivalence relation $\sim$ on a set A and element $a \in A$, the *equivalence class of* a is the set

$$[a] = \{b \in A : b \sim a\}.$$

Any element $b \in [a]$ is called a *representative* of $[a]$. We denote the set of all equivalence classes of $\sim$ by $A/\sim$, referring to it as the *quotient of* A *by* $\sim$.

If you stick with a career in mathematics, you will see equivalence classes arise over and over in an almost infinite variety of contexts.

The equivalence classes of an equivalence relation $\sim$ on A form a partition of A. That is,

- for every $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$;
- $\bigcup_{a \in A} [a] = A$.

Since $a \in [a]$, the second item is clear. To see that the first item holds, suppose $[a] \cap [b] \neq \emptyset$, and let c be an element of the intersection. Then $a \sim c$ and $b \sim c$, so by transitivity (and symmetry!) $a \sim b$. But if this is true, then for any $c' \in [b]$, we have $b \sim c'$ implies $a \sim c'$ again by transitivity.

This shows that $[b] \subset [a]$. Exactly the same reasoning gives $[a] \subset [b]$. Hence $[a] \cap [b] \neq \emptyset$ implies $[a] = [b]$, as desired.

Recall example **??** above. We call the equivalence classes for this equivalence relation "rational numbers", generally writing p/q instead of $[(p, q)]$. We denote the set of all such equivalence classes by . That's where that example comes from.

The following are (well-defined) operations on .

- $p/q + r/s = (ps + rq)/qs$.
- $p/q \cdot r/s = pr/qs$.

Together with these operations, is field.

Whenever anyone asserts that 'such and such a function is well-defined', they really mean that it's clearly a relation but not so clearly a function. This happens often with functions that act on equivalence classes. The point is that to describe the function one must almost always do so in terms of representatives of equivalence classes rather than the classes themselves. And since representatives of a class are rarely unique, one must show that changing the representative of the class does not change the value of the function. For example, if addition is to be a well-defined operation, then $2/3 + 9/1557/45$ better be the same rational number as $4/6 + 3/538/30$.

So let's show that '$\cdot$' is well-defined. Suppose that (p', q') is another representative (i.e. other than (p, q)) of the class p/q. Then $pq' = p'q$. The point is to show that $(p'r, q's)$ is another representative of the class pr/qs. That is, we must verify

$$prq's = p'rqs.$$

This is easily done by multiplying $pq' = p'q$ through by rs. Verifying that $+$ is well-defined and that $\cdot$, $+$ satisfy the field axioms is your problem.

There's one other kind of relation that we'll touch on here. wouldn't be complete without a relation of this sort, and as we'll see, falls short of being complete even with it.

A relation $<$ on a set A is a called a *(total) order* if

- it is transitive, and
- for every $a, b \in A$, exactly one of the following holds:

$$a = b, \quad a < b, \quad b < a$$

The standard order relation on is given by $p/q < r/s$ if and only if $ps < rq$. As with addition and multiplication, one (that one being you) needs to check that this definition doesn't depend on which representative we're using. Another thing to check is that arithmetic and order cooperate on .

Together with the operations $+$ and $\cdot$ and the order $<$, the set is an ordered field. That is, in addition to being a field with an order,

- $x < y$ implies $x + z < y + z$,
- $x, y > 0$ implies $xy > 0$,

for every $x, y, z \in$.

We deal only with the first item. Write $x = p/q$, $y = r/s$. Then $ps < qr$. Write $z = m/n$. Then $x + z = (pn + mq)/nq$ and $y + z = (rn + ms)/ns$. Thus we check

$$\begin{aligned}(pn + mq)ns - (rn + ms)nq &= n(pns + mqs - rnq - msq) \\ &= n^2(ps - qr) < 0\end{aligned}$$

since $n^2 > 0$. We conclude that $x + z < y + z$.

Of course we always think of the integers as being a subset of the rationals. This is maybe less clear given our definition of the rationals as equivalence classes of a relation on $\times^+$ (how on earth can be a subset of *that*?). The precise meaning of $\subset$ is

Let $\iota :\rightarrow$ be the function $i(m) = m/1$. Then ι is injective and preserves order and arithmetic. That is, for every $m, n \in$

- $m < n$ if and only if $\iota(m) < \iota(n)$;
- $\iota(m + n) = \iota(m) + \iota(n)$;
- $\iota(mn) = \iota(m)\iota(n)$.

The proof of this theorem is straightforward and left to you. Note that in mathematical parlance, injective functions of one set into another that also have the happy property of respecting all mathematical operations, orders, etc that one happens to care about at the moment are said to be *isomorphisms onto their images.*