Natural numbers, integers, rationals

Equivalence relation on a set

Let A be a set. A binary relation on A is a subset R of $A \times A$.

We write $a \sim b$ (a is related to b) if $(a, b) \in R$.

We shall be interested in a special type of relation called the equivalence relation.

A relation $\sim$ on A is called an equivalence relation if the following three conditions hold:

1. $x \sim x$ for all $x \in A$.

2. For $x, y \in A$, if $x \sim y$, then $y \sim x$.

3. For $x, y, z \in A$ if $x \sim y$ and $y \sim z$ hold, then $x \sim z$.

One of the most important results in this context:

Theorem. Let A be a set. An equivalence relation $\sim$ on A partitions A into disjoint subsets. (Converse is also true.)

Proof. For $a \in A$, write

$$[a] := \{x \in A \,|\, x \sim a\},$$

called the *equivalence class* of a.

Clearly,

$$A = \bigcup_{a \in A} [a]$$

Check that the equivalence classes are either equal or disjoint.

Conversely, let

$$A = \bigcup_{\alpha \in I} A_\alpha,$$

be a partition of A into disjoint subsets.

Define: $a \sim b$ if and only if there is some $\alpha \in I$ such that $a, b \in A_\alpha$. Check that this is an equivalence relation. ∎

A construction

For any set A, define $S(A) = A \cup \{A\}$. This is called the <u>successor operation</u>. Let us now apply this operation repeatedly, starting from:

$$\emptyset$$

The empty set!

Starting point: $\emptyset$.

$S(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$.

$S(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$.

$S(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

$S(-) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$.

... and so on...

Let us give those sets from the last page some names (rather symbols).

Write:

0 for $\emptyset$.

1 for $\{\emptyset\} \quad (= \{0\})$.

2 for $\{\emptyset, \{\emptyset\}\} \quad (= \{0, 1\})$.

3 for $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \quad (= \{0, 1, 2\})$.

4 for $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$ $(= \{0, 1, 2, 3\})$.

... and so on ...

The system of symbols $\{0, 1, 2, 3, 4, 5, \cdots\}$ thus obtained is the set of natural numbers, denoted by $\mathbb{N}$.

Remark 1: Each natural number is a set.

Remark 2: A natural number is the set of its preceding natural numbers.

The set $\mathbb{N}$ satisfies the so called Peano Axioms:

- 0 is a natural number.
- Every natural number has a successor which is also a natural number.
- 0 is not the successor of any natural number.

- If the successor of x equals the successor of y, then x equals y.

- (Axiom of Induction) If a statement is true for 0, and if the truth of that statement for a number implies its truth for the successor of that number, then the statement is true for every natural number.

Addition.

Define $n + 0 = n$ for all n. Then go on recursively as follows:

$$n + S(m) = S(n + m)$$

Illustration:

$$1 + 1 = 1 + S(0) := S(1 + 0) = S(1) = 2$$

$$2 + 1 = 2 + S(0) := S(2 + 0) = S(2) = 3$$

$$n + 1 = n + S(0) := S(n + 0) = S(n)$$

Remark: Note that $n+1$ is the successor of n.

The set $\mathbb{N}$, together with addition $+$ satisfies:

1. $n+(m+p) = (n+m)+p$ for all $m, n, p \in \mathbb{N}$.

2. $n + m = m + n$ for all $m, n \in \mathbb{N}$.

3. $n + 0 = n$ for all $n \in \mathbb{N}$.

Exercise: Prove the above properties!

In an algebraic system as above we would like to solve equations.

While the equation $X + 1 = 2$ has a solution in $\mathbb{N}$, the following

$$X + 2 = 1$$

does not (why?).

Question. Can we embed $\mathbb{N}$ in a bigger system, retaining all its properties, so that the equation as above has a solution (in the bigger system)?

So we have to bring in the "negatives". We only have $(\mathbb{N}, +)$ and basic set theory at our disposal. This will be our focus now.

Construction of Integers

Consider the set $X = \mathbb{N} \times \mathbb{N}$. On X, define the relation:

$$(a, b) \sim (c, d) \text{ if } a + d = c + b$$

Example. $(1, 3) \sim (5, 7)$, $(11, 5) \sim (100, 94)$ etc.

Exercise. Check that $\sim$ is an equivalence relation.

Write $\mathbb{Z}$ = set of all equivalence classes.

Notation: $[(a, b)]$ for the equivalence class containing (a, b).

Now define addition on these equivalence classes:

$$[(a, b)] \oplus [(m, n)] := [(a + m, b + n)]$$

(note that $+$ is from $\mathbb{N}$)

Remark. What if $[(a,b)] = [(c,d)]$ and $[(m,n)] = [(p,q)]$? Do we have

$$[(a,b)] \oplus [(m,n)] = [(c,d)] \oplus [(p,q)]?$$

Let us check.
$[(a,b)] = [(c,d)] \Rightarrow (a,b) \sim (c,d)$
$(a,b) \sim (c,d) \Rightarrow a + d = c + b$
$[(m,n)] = [(p,q)] \Rightarrow (m,n) \sim (p,q)$
$(m,n) \sim (p,q) \Rightarrow m + q = p + n$

Then, $a+d+m+q = c+b+p+n$ and therefore, $\underline{a+m} + \underline{d+q} = \underline{c+p} + \underline{b+n}$, implying $(a+m, b+n) \sim (c+p, d+q)$. In other words,

$$[(a,b)] \oplus [(m,n)] = [(c,d)] \oplus [(p,q)],$$

and the definition is consistent.

What is the "zero" in $\mathbb{Z}$?

It is the class of $(0,0)$ (which is the same as $[(1,1)], [(2,2)], [(3,3)], \cdots$).

The natural numbers are embedded in $\mathbb{Z}$ as follows:

$$f : \mathbb{N} \longrightarrow \mathbb{Z} \text{ by}$$

$$n \mapsto [(n,0)]$$

Exercise: Prove that f is injective.

Do we have some $[(a,b)] \in \mathbb{Z}$ such that

$$[(a,b)] \oplus [(1,0)] = [(0,0)] \text{ ?}$$

Yes, $[(0,1)] \oplus [(1,0)] = [(1,1)] = [(0,0)]$.

In general, $[(0,n)] \oplus [(n,0)] = [(n,n)] = [(0,0)]$.

Let us call $[(n,0)]$ as n and $[(0,n)]$ as $-n$. These are the negatives.

Let us now drop the $\oplus$ notation. Also, write n for $[(n, 0)]$ and $-n$ for $[(0, n)]$.

Take any integer $[(a, b)] \in \mathbb{Z}$.

Then

$$[(a, b)] = [(a, 0)] + [(0, b)] = a - b$$

Thus, we realized integers as difference of natural numbers.

On $\mathbb{N}$. we can also define multiplication.

Define $n \times 0 = 0$ for all n.

Then,

$$n \times S(m) = n \times m + n$$

You can easily check the properties of multiplication and the distributive law.

You can extend this definition to $\mathbb{Z}$.

Now that we have addition and multiplication on $\mathbb{Z}$, consider the equation:

$$2x = 3$$

It has no solution in $\mathbb{Z}$.

Again, can we embed $\mathbb{Z}$ into some bigger structure where we have a solution?

If we can accommodate reciprocals of $n \in \mathbb{Z} \setminus \{0\}$, we shall be done.

Almost a similar construction as before.

Take

$$X = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \,|\, b \neq 0\}$$

Define a relation $\sim$ on X by:

$$(a, b) \sim (c, d) \text{ iff } ad = bc$$

Check that this is an equivalence relation.

Define $\mathbb{Q} = X/\sim$ (the set of equivlence classes).

Notation: write $[(a, b)]$ for the equivalence class of (a, b).

Define:

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

$$[(a, b)] \times [(c, d)] = [(ac, bd)]$$

Exercise: Check that the above operations are well-defined.

Take any $[(a,b)] \in \mathbb{Q}$, with $a \neq 0$. Then

$$[(a,b)] \times [(b,a)] = [(ab,ab)] = [(1,1)]$$

Let us keep this in mind.

For convenience, we write $[(a,b)]$ as $\frac{a}{b}$.

We have an injective map

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Q}$$

$$n \mapsto \frac{n}{1}$$

Therefore, we can identify $\frac{n}{1}$ of $\mathbb{Q}$ with n.

Let $n(\neq 0) \in \mathbb{Z}$. Note that, in $\mathbb{Q}$ we have

$$\frac{n}{1} \times \frac{1}{n} = \frac{1}{1}$$

In other words, n has reciprocal in $\mathbb{Q}$.

Now consider the equation:

$$x^2 = 2$$

This has no solution in $\mathbb{Q}$.

One then constructs $\mathbb{R}$ to tackle this problem.

But this construction is not an algebraic one as the above two.

That's analysis.

Again, another equation! Consider

$$x^2 + 1 = 0$$

This has no solution in $\mathbb{R}$.

How do we embed $\mathbb{R}$ into a bigger structure?

We shall take

$$\frac{\mathbb{R}[X]}{\langle X^2 + 1 \rangle},$$

where

$$\langle X^2 + 1 \rangle = \{(X^2 + 1)f(X) \mid f(X) \in \mathbb{R}[X]\}$$

(i.e. all multiples of $X^2 + 1$).

Let us call $\frac{\mathbb{R}[X]}{\langle X^2+1 \rangle}$ as $\mathbb{C}$.

We shall see later that:

- there is a natural injection $\varphi : \mathbb{R} \longrightarrow \mathbb{C}$;

- -1 has a square root in $\mathbb{C}$.

And this construction of $\mathbb{C}$ would be the model for various such general constructions.