MATH 5615H – HONORS ANALYSIS I

9/4/2019

We assume that we are given the set of natural numbers

$$\mathbb{N} = \{0, 1, 2, \dots, n, \dots\},$$

together with the two operations of addition and multiplication, which are both associative and commutative. The purpose of these notes is to construct from here the integers and the rationals as successive extensions of the concept of "number".

Relations

Definition 1. Let S be a set. A *relation R on S* is a subset $R \subset S \times S$. For $x, y \in S$, we write xRy if $(x, y) \in R$.
The relation R is called

- *reflexive*, if $xRx, \forall\, x \in S$.
- *symmetric*, if xRy implies yRx.
- *antisymmetric*, if xRy and yRx imply together that $x = y$.
- *transitive*, if xRy and yRz imply together that xRz.

A relation which is reflexive, symmetric, and transitive is called an *equivalence* relation (usually we'll denote equivalence relations by "$\sim$").
A relation which is reflexive, antisymmetric, and transitive is called a *(partial) ordering* (usually denoted by "$\leq$"). $(S, \leq)$ is called a partially ordered set. It is *totally ordered* if $\forall\, x, y \in S$ we have either $x \leq y$, or $y \leq x$, i.e., any two elements of S are comparable.

Examples of partial order relations: 1) $(\mathbb{N}, \leq)$ is totally ordered. Here, the usual order relation "$\leq$" on $\mathbb{N}$ is defined in terms of the addition operation as follows:

Given $a, b \in \mathbb{N}$, we say that $a \leq b$ iff there is a $c \in \mathbb{N}$ with $b = a + c$.

2) Consider on $\mathbb{N}$ the *divisibility relation* $a|b$ iff there is a $c \in \mathbb{N}$ with $b = ac$. Then $(\mathbb{N}, |)$ is only partially ordered.

3) The subsets of a given set form a partially ordered set with respect to inclusion.

In keeping with the usage in Rudin's book, from now on by an ordered set we will mean a *totally ordered* set.

Examples of equivalence relations: 1) The "$=$" relation on any set S.

2) The so-called "cardinal equivalence" relation on sets. This will appear at the beginning of Chapter II in Rudin's book. If A, B are sets, we say that A is equivalent to B, and write $A \sim B$, iff there exists a mapping $f : A \longrightarrow B$ which is bijective. You should check for yourselves that this is indeed an equivalence relation.

3) Let $f : S \longrightarrow T$ be a function. Define a relation $\sim_f$ on S by

$$x \sim_f y \text{ iff } f(x) = f(y).$$

It is immediate to check that "$\sim_f$" is an equivalence relation.

Our next task is to show that *all* equivalence relations are of the kind described in Example 3 above. So let $S \neq \emptyset$ be any set and let "$\sim$" be an equivalence relation on S. Call a subset $\emptyset \neq C \subset S$ an *equivalence class* (of "$\sim$" on S) if it satisfies

(a) $x \sim y$, $\forall\, x, y \in C$

(b) if for $z \in S$ there is an $x \in C$ such that $x \sim z$, then $z \in C$.

Note that for any $x \in S$ there is an equivalence class containing it, namely

$$C_x := \{y \in S \mid y \sim x\}.$$

(It is trivial to check that C_x satisfies (a) and (b).)

Let now C_1, C_2 be two equivalence classes. Then

Claim : Either $C_1 \cap C_2 = \emptyset$, or $C_1 = C_2$.

Proof: If $C_1 \cap C_2 \neq \emptyset$, let $x \in C_1 \cap C_2$. Pick $y \in C_1$. Then $x \sim y$ by (a) for C_1, so $y \in C_2$ by (b) for C_2. Hence $C_1 \subset C_2$. The reverse inclusion follows similarly.

We deduce from the above discussion that S is the disjoint union of all the equivalence classes. Now put

$$T := \text{ the set of equivalence classes of " } \sim \text{ " on } S$$

and define $p : S \longrightarrow T$ by $p(x) = C_x$. It follows that p is a well-defined surjective map, and it is clear from the construction that $\sim$ coincides with $\sim_p$.

Definition 2. T is called the *quotient of S by $\sim$*, and p is called the *canonical surjection.* Usually we will write $S/\sim$ instead of T for the quotient set.

A *complete set of representatives* for the quotient set is a subset $\{x_i\}_{i \in I} \subset S$ such that $T = \cup_{i \in I} C_{x_i}$ and $C_{x_i} \neq C_{x_j}$ for $i \neq j$.

Construction of the integers

Recall that on $\mathbb{N}$ we have the *partially defined* operation of subtraction: given $a, b \in \mathbb{N}$, with $a \leq b$, let $c \in \mathbb{N}$ be such that $b = a + c$ and *define*

$$b - a := c.$$

The idea is now to enlarge our notion of number by inventing new numbers which are the "result of the subtraction $b - a$" even when $a > b$!

Let $S := \mathbb{N} \times \mathbb{N}$. We introduce a relation $\sim$ on S as follows:

$$(a, b) \sim (a', b') \text{ iff } a + b' = a' + b.$$

(Secretly, we think of the equation $a + b' = a' + b$ to mean $a - b = a' - b'$, even though the subtraction doesn't yet make sense always.)

It is very easy to check that $\sim$ is an equivalence relation on S.

Definition 3. The set of *integers* is the quotient set

$$\mathbb{Z} := S/\sim.$$

So an element of $\mathbb{Z}$ is an equivalence class of pairs of natural numbers. Given $(a,b) \in \mathbb{N} \times \mathbb{N}$, we denote $\widehat{(a,b)} = C_{(a,b)}$ the equivalence class containing it.

You should convince yourselves that a complete set of representatives is given by

$$\{\dots, (0,m), \dots, (0,2), (0,1), (0,0), (1,0), (2,0), \dots, (n,0), \dots\},$$

so that

$$\mathbb{Z} = \{\dots, \widehat{(0,m)}, \dots, \widehat{(0,2)}, \widehat{(0,1)}, \widehat{(0,0)}, \widehat{(1,0)}, \widehat{(2,0)}, \dots, \widehat{(n,0)}, \dots\}$$

Next we define addition and multiplication operations $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ and $\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ by the formulas:

$$\widehat{(a,b)} + \widehat{(c,d)} = \widehat{(a+c, b+d)},$$

$$\widehat{(a,b)} \cdot \widehat{(c,d)} = \widehat{(ac+bd, ad+bc)}.$$

Precisely, this means the following. Given $x, y \in \mathbb{Z}$, pick representatives (a,b) for x, respectively $c,d)$ for y. Then we define the sum $x+y$ to be the equivalence class containing $(a+c, b+d)$ and the product $x \cdot y$ to be the equivalence class containing $(ac+bd, ad+bc)$.

Lemma 1. Addition and multiplication are well-defined operations on $\mathbb{Z}$
Proof: We need to check that they do not depend on the chosen representatives of the equivalence classes. Assume that $(a,b) \sim (a',b')$, i.e., $a+b' = a'+b$, and that $(c,d) \sim (c',d')$, i.e., $c+d' = c'+d$. We have

$$(a+c)+(b'+d') = (a+b')+(c+d') = (a'+b)+(c'+d) = (a'+c')+(b+d),$$

which means precisely that $(a+c, b+d) \sim (a'+c', b'+d')$. Hence we've shown that $\widehat{(a,b)} + \widehat{(c,d)} = \widehat{(a',b')} + \widehat{(c',d')}$.

For multiplication, it is better to proceed in two steps: first show that $\widehat{(a,b)} \cdot \widehat{(c,d)} = \widehat{(a',b')} \cdot \widehat{(c,d)}$, and then show similarly that $\widehat{(a',b')} \cdot \widehat{(c,d)} = \widehat{(a',b')} \cdot \widehat{(c',d')}$. I'll leave this as an exercise.

Proposition 1. Addition and multiplication on $\mathbb{Z}$ satisfy the following properties:
(i) addition is associative: $(x+y)+z = x+(y+z), \forall x,y,z \in \mathbb{Z}$;
(ii) $\mathbb{Z}$ contains an element 0 such that $0+x = x+0 = x, \forall x \in \mathbb{Z}$;
(iii) $\forall x \in \mathbb{Z}$, there is an element $-x \in \mathbb{Z}$, such that $x+(-x) = (-x)+x = 0$;
(iv) addition is commutative: $x+y = y+x, \forall x,y \in \mathbb{Z}$;
(v) multiplication is associative: $(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x,y,z \in \mathbb{Z}$;
(vi) $\mathbb{Z}$ contains an element 1 such that $1 \cdot x = x \cdot 1 = x, \forall x \in \mathbb{Z}$;
(vii) multiplication is commutative: $x \cdot y = y \cdot x, \forall x,y \in \mathbb{Z}$;
$(viii)$ multiplication is distributive with respect to addition:

$$x \cdot (y+z) = x \cdot y + x \cdot z, \forall x,y,z \in \mathbb{Z}.$$

Proof:

(i) and (iv) Write $x = \widehat{(a,b)}, y = \widehat{(c,d)}, z = \widehat{(e,f)}$, with $a,b,c,d,e,f \in \mathbb{N}$. Then

$$(x+y)+z = \widehat{((a+c)+e, (b+d)+f)} = \widehat{(a+(c+e), b+(d+f))} = x+(y+z),$$

the middle equality by the associativity of addition in $\mathbb{N}$. Similarly,

$$x + y = \widehat{(a + c, b + d)} = \widehat{(c + a, d + b)} = y + x.$$

(ii) Take $0 = \widehat{(0,0)}$. Pick $x \in \mathbb{Z}$ and write $x = \widehat{(a,b)}$. Clearly $0 + x = \widehat{(0 + a, 0 + b)} = \widehat{(a,b)} = x$.

(iii) Given $x = \widehat{(a,b)}$, put $-x = \widehat{(b,a)}$. Then $x + (-x) = \widehat{(a + b, b + a)} = \widehat{(0,0)} = 0$.

(v) and (vii) I will leave as exercises.

(vi) Take $1 = \widehat{(1,0)}$. Then $1 \cdot x = \widehat{(1a + 0b, 1b + 0a)} = \widehat{(a,b)} = x$.

$(viii)$ Again, write $x = \widehat{(a,b)}, y = \widehat{(c,d)}, z = \widehat{(e,f)}$, with $a,b,c,d,e,f \in \mathbb{N}$. We have

$$\begin{aligned} x \cdot (y + z) =& \widehat{(a,b)} \cdot \widehat{(c + e, d + f)} = \\ & \widehat{(a(c+e) + b(d+f), a(d+f) + b(c+e))} = \\ & \widehat{((ac + bd) + (ae + bf), (ad + bc) + (af + be)))} = \\ & \widehat{(ac + bd, ad + bc)} + \widehat{(ae + bf, af + be)} = \\ & \widehat{(a,b)} \cdot \widehat{(c,d)} + \widehat{(a,b)} \cdot \widehat{(e,f)} = \\ & x \cdot y + x \cdot z. \end{aligned}$$

Remark/Definition. The algebraic structure described above is a very important one in many areas of mathematics and so it has its own name. Namely, a set R endowed with two internal operations $+ : R \times R \longrightarrow R$ and $\cdot : R \times R \longrightarrow R$ which satisfy axioms (i) through $(viii)$ of Proposition 1 is called a *commutative ring*. Note that in any commutative ring R (in particular, in $\mathbb{Z}$), we have a well-defined subtraction operation, by setting

$$x - y := x + (-y), \forall x, y \in R.$$

The commutative ring $\mathbb{Z}$ has one additional property, namely

$$\text{If } xy = 0, \text{ then } x = 0 \text{ or } y = 0.$$

(Exercise: Prove this!) A commutative ring satisfying this additional requirement is called an integral domain. We will not use these general notions in this course.

We introduce also an order relation on $\mathbb{Z}$ as follows: If $x = \widehat{(a,b)}, y = \widehat{(c,d)}$, we say that $x \leq y$ if and only if $a + d \leq b + c$. It is immediate to check that this is a total order. If we choose the system of representatives discussed earlier, we have

$$\{\cdots \leq \widehat{(0,m)} \leq \cdots \leq \widehat{(0,2)} \leq \widehat{(0,1)} \leq \widehat{(0,0)} \leq \widehat{(1,0)} \leq \widehat{(2,0)} \leq \cdots \leq \widehat{(n,0)} \leq \dots\}$$

Define a mapping

$$\phi : \mathbb{N} \longrightarrow \mathbb{Z}, \quad \phi(n) = \widehat{(n,0)}.$$

The map ϕ is obviously injective. It is immediate to check that ϕ respects the two operations on $\mathbb{N}$ and $\mathbb{Z}$, that is,

$$\phi(n+m) = \phi(n) + \phi(m), \quad \phi(mn) = \phi(m) \cdot \phi(n).$$

Identifying $\mathbb{N}$ with its image in $\mathbb{Z}$ via ϕ allows us to view $\mathbb{N}$ as a subset of $\mathbb{Z}$, such that the operations and the order relation on $\mathbb{Z}$ extend those on $\mathbb{N}$, and we will always make this identification from now on. Accordingly, we change notation one last time and put $n = \widehat{(n,0)}$ for each $n \in \mathbb{N}$. Since we have $-\widehat{(n,0)} = \widehat{(0,n)}$ (see the proof of (iii) in Proposition 1), we also denote $-n = \widehat{(0,n)}$ for $n \geq 1$. We will call $-n$ a *negative integer*. Now the set $\mathbb{Z}$ we have just constructed is the familiar

$$\mathbb{Z} = \{\cdots \leq -m \leq \cdots \leq -2 \leq -1 \leq 0 \leq 1 \leq \cdots \leq n \leq \dots\},$$

with all its standard structures.

Construction of the rationals

One deficiency of $\mathbb{Z}$ is the fact that the operation of *division* is only partially defined. However, now we have a clear roadmap on how to fix this.

Let $\mathbb{Z}^* = \mathbb{Z} - \{0\}$. Denote $S = \mathbb{Z} \times \mathbb{Z}^*$. Define a relation $\sim$ on S by

$$(m,n) \sim (k,l) \text{ iff } ml = kn.$$

It is immediate to check this is an equivalence relation.

Definition 4. The set of *rational numbers* is the quotient set

$$\mathbb{Q} := S/\sim .$$

We denote by $\frac{m}{n} = C_{(m,n)}$ the equivalence class of the pair $(m,n) \in S$.

We define the addition and multiplication operations on $\mathbb{Q}$ by the formulas

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Lemma 2. Addition and multiplication are well-defined operations on $\mathbb{Q}$.
Proof: Exercise.

Definition 5. Let F be a set endowed with two internal operations, addition $+ : F \times F \longrightarrow F$, and multiplication $\cdot : F \times F \longrightarrow F$. We say that F is a field if the two operations satisfy axioms (i) through $(viii)$ of Proposition 1, and one additional axiom,

(ix) for every $0 \neq x \in F$, there is an element $x^{-1} \in F$ such that $xx^{-1} = 1$. Sometimes x^{-1} is also denoted $1/x$. I will use both notations interchangeably.

Proposition 2. $(\mathbb{Q}, +, \cdot)$ is a field.
Proof: Exercise (take $0 = \frac{0}{1}$, $1 = \frac{1}{1}$, $-\left(\frac{m}{n}\right) = \frac{-m}{n}$, and $\left(\frac{m}{n}\right)^{-1} = \frac{n}{m}$).

Definition 6. An element $x \in \mathbb{Q}$ is called a *positive rational number* if it has a representative $x = \frac{m}{n}$ with both m and n positive integers. In this case, we write $x > 0$. Further, we say that $x \geq 0$ if either $x > 0$, or $x = 0$.

Given $x, y \in \mathbb{Q}$, we say that $x \leq y$ iff $y - x \geq 0$.

An element $x \in \mathbb{Q}$ is called a *negative rational number* if $-x > 0$. In this case, we also write $x < 0$.

Proposition 3. The relation "$\leq$" defined above is an order on $\mathbb{Q}$. (Recall that order means total order for us.)
Proof: Exercise.

Proposition 4. The map $\psi : \mathbb{Z} \longrightarrow \mathbb{Q}, \psi(n) = \frac{n}{1}$ is injective and satisfies

$$\psi(m+n) = \psi(m) + \psi(n), \quad \psi(mn) = \psi(m)\psi(n).$$

Further, $m \leq n$ iff $\psi(m) \leq \psi(n)$.
Proof: Exercise.

As before, identifying $\mathbb{Z}$ with its image $\psi(\mathbb{Z})$ allows us to view $\mathbb{Z}$ as a subset of $\mathbb{Q}$, and we will do so without comment from now on.