UM 204 (WINTER 2024)

What is this course about? We will lay a rigorous foundation for the rules of calculus. The purpose of this course is to familiarize the audience with the kind of abstract thinking that is needed to study modern analysis. We will assume

- basic results of set theory;
- the existence of the set of natural numbers

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

  with the usual operations of addition & multiplication.

For an axiomatic (but readable) approach See Halmos' *Naive Set Theory* or Tao's *Analysis 1*, Chapter 2. For those who attended UM 101 in 2022-23, see the first three lectures of the UM 101 notes.

1. Integers and rational numbers

1.1. **Brief recap of natural numbers.** We had defined the set of natural numbers as the unique minimal inductive set granted by the ZFC axioms. By the recursion principle (also granted by the ZFC axioms), we defined addition and multiplication on $\mathbb{N}$ and showed that these operations

(1) are commutative & associative,
(2) admit identities (0 and 1, respectively)
(3) satisfy the appropriate distribution law, and
(4) satisfy the cancellation law.

Most elements, however, do not admit inverses under either operations. This is addressed by the construction of integers and rational numbers.

1.2. **Relations on sets.** A relation R on a set A is a subset of $A \times A$. We write xRy to denote that $(x, y) \in R$.

Definition 1.1. A partial order on a set A is a relation R satisfying

(1) reflexivity, i.e., xRx for all $x \in A$,
(2) anti-symmetry, i.e., if xRy and yRx, then $x = y$, for all $x, y \in A$, and
(3) transitivity, i.e., xRy and yRz implies that xRz for all $x, y, z \in A$.

In this case, the pair (A, R) is called a partially ordered set, or poset. Additionally, if

(4) for each $x, y \in A$, either xRy or yRx,

then R is called an order (or total order) and (A,R) is an ordered set, or totally ordered set.

Partial orders are generally denoted by $\leq$ instead of R. In UM 101, we had defined “order" slightly differently— by imposing that xRy and yRx cannot occur simultaneously. We will refer to that notion as a *strict order*, and denote it by $<$. Every order corresponds to a strict order, and vice versa. Check.

Example 1. Given $m,n \in \mathbb{N}$, we say that $m \leq n$ if there exists a $k \in \mathbb{N}$ such that $m+k=n$. Recall that $(\mathbb{N},\leq)$ is an ordered set. Moreover, addition and multiplication by natural numbers preserve order.

Definition 1.2. An equivalence relation on a set A is a relation R satisfying

(1) reflexivity,
(2) symmetry, i.e., $xRy \iff yRx$ for all $x,y \in A$, and
(3) transitivity.

Given an equivalence relation R on A and $x \in A$, the equivalence class of x is the set

$$[x]_R = \{y \in A : xRy\}.$$

The collection $\{[x]_R : x \in A\}$ partitions the set A. Check.

1.3. **Integers.** One cannot solve equations of the form

$$3+x=2$$

within $\mathbb{N}$. Check. Our desire to “subtract" can be formalized by using equivalence relations.

Consider the relation on $\mathbb{N}\times\mathbb{N}$ given by

$$(a,b)R(c,d) \iff a+d=b+c.$$

Definition 1.3. The set of equivalence classes of R is called the set of integers, and is denoted by $\mathbb{Z}$. Let

$$[(a,b)]+_{\mathbb{Z}}[(c,d)] = [(a+c,b+d)]$$

$$[(a,b)]\cdot_{\mathbb{Z}}[(c,d)] = [(ac+bd,ad+bc)]$$

We say that $[(a,b)] \leq_{\mathbb{Z}} [(c,d)]$ if there is a natural number $n \in \mathbb{N}$ such that $[(a,b)] +_{\mathbb{Z}} [(n,0)] = [(c,d)]$.

END OF LECTURE 1

First, we need make sure that the operations defined above are well-defined. As a sample, we prove that $+_{\mathbb{Z}}$ is well-defined. We need to show that if $(a,b)R(a',b')$ and $(c,d)R(c',d')$, then

$$(a+c,b+d)R(a'+c',b'+d').$$

This is true because

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

□

Theorem 1.4. (*a*) $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, \leq_{\mathbb{Z}})$ *is an ordered commutative ring, i.e., the following hold.*

(R1) $+_{\mathbb{Z}}$ *and* $\cdot_{\mathbb{Z}}$ *are commutative and associative on* $\mathbb{Z}$.

(R2) *For every* $z \in \mathbb{Z}$, $z +_{\mathbb{Z}} [(0,0)] = z$ *and* $z \cdot_{\mathbb{Z}} [(1,0)] = z$.

(R3) *Given* $z \in \mathbb{Z}$, *there is a (unique)* $y \in \mathbb{Z}$ *such that* $z +_{\mathbb{Z}} y = [(0,0)]$. *Define* $-z$ *to be this unique* y. *Given* $z, w \in \mathbb{Z}$, *define* $z - w$ *to be* $z + (-w)$.

(R4) $\cdot_{\mathbb{Z}}$ *distributes over* $+_{\mathbb{Z}}$.

(O5) $(\mathbb{Z}, \leq_Z)$ *is an ordered set.*

(OR6) *If* $z \leq_{\mathbb{Z}} w$, *then* $z +_{\mathbb{Z}} u \leq_{\mathbb{Z}} w +_{\mathbb{Z}} u$ *for all* $z, u, w \in \mathbb{Z}$.

(OR7) *If* $0 \leq_{\mathbb{Z}} z, w$, *then* $0 \leq_{\mathbb{Z}} z \cdot_{\mathbb{Z}} w$ *for all* $z, w \in \mathbb{Z}$.

(*b*) *The map* $f : \mathbb{N} \to \mathbb{Z}$ *given by* $n \mapsto [(n,0)]$ *is injective and respects addition, multiplication and order: i.e., for all* $m, n \in \mathbb{N}$,

- $f(m+n) = f(m) +_{\mathbb{Z}} f(n)$,
- $f(m \cdot n) = f(m) \cdot_{\mathbb{Z}} f(n)$,
- $m \leq n \iff f(m) \leq f(n)$.

Thus, we may view $(\mathbb{N}, +, \cdot, \leq)$ as a subset of $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, \leq_{\mathbb{Z}})$. Denote $[(n,0)]$ by n, and drop $\mathbb{Z}$ in the subscript. We have that $-[(a,b)] = [(b,a)]$, and therefore, $[(a,b)] = [(a,0)] + [(b,0)] = a - b$. One often denotes $[(a,b)]$ by $a - b$.

We note (but don't prove) that $\mathbb{Z}$ satisfies many additional properties that we are accustomed to, e.g., $\mathbb{Z}$ lacks zero divisors; cancellation laws for + and $\cdot$; trichotomoy, i.e., each $z \in \mathbb{Z}$ is either n or $-n$ for some $n \in \mathbb{N}$.

1.4. Rational numbers.

One cannot solve equations of the form

$$3x = 2$$

within $\mathbb{Z}$ (Check). Our desire to "divide" can also be formalized by using equivalence relations.

Let $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Consider the relation on $\mathbb{Z} \times \mathbb{Z}^*$ given by

$$(a,b)R(c,d) \iff ad = bc.$$

Definition 1.5. The set of equivalence classes of R is called the set of rational numbers, and is denoted by $\mathbb{Q}$. Let, for $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}^*$,

$$[(a,b)] +_{\mathbb{Q}} [(c,d)] = [(ad + bc, bd)],$$

$$[(a,b)] \times_{\mathbb{Q}} [(c,d)] = [(ac, bd)].$$

We say that $[(a,b)] \leq_{\mathbb{Q}} [(c,d)]$ if $(bc-ad)(bd) \geq 0$.

Theorem 1.6. *(a)* $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, \leq_{\mathbb{Q}})$ *is an ordered field (recap definition & properties from UM 101), with*

(1) $0 = [(0,1)]$,
(2) $1 = [(1,1)]$,
(3) $-[(a,b)] = [(-a,b)]$, *Given $z, w \in \mathbb{Z}, w \neq 0$, define $z - w$ to be $z +_{\mathbb{Q}} (-w)$.*
(4) $1/[(a,b)] = [(b,a)]$ *whenever $a \neq 0$. Given $z, w \in \mathbb{Z}, w \neq 0$, define z/w to be $z \cdot_{\mathbb{Q}} \frac{1}{w}$.*

(b) The map $a \mapsto [(a,1)]$ is an ordered ring isomorphism from $(\mathbb{Z}, +, \times, \leq)$ onto a subset of $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, \leq_{\mathbb{Q}}$).As before, if we denote $[(a,1)]$ by a, then $[(a,b)] = a/b$, and we use the latter to denote this class.

END OF LECTURE 2

Another important operation on $\mathbb{N}$ (granted by the recursion principle) is exponentiation, i.e., there is a function pow : $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that

(1) $\text{pow}(m,0) = 1$ for all $m \in \mathbb{N}$, and
(2) $\text{pow}(m,n+1) = m\text{pow}(m,n)$ for all $m,n \in \mathbb{N}$.

Using the fact that any $m \in \mathbb{Z}$ is either n or $-n$ for some $n \in \mathbb{N}$, we extend the above function to $\mathbb{Q}^* \times \mathbb{Z}$:

$$\text{pow(a/b,m)} = \begin{cases} a^n/b^n, & \text{if } m = n, n \in \mathbb{N}, \\ b^n/a^n, & \text{if } m = -n, n \in \mathbb{N}. \end{cases}$$

The above definition is well-defined. We denote $\text{pow}(m,n)$ more commonly by m^n, and it satisfies the usual properties of exponentiation. Read Tao's Section 4.3 on absolute value and exponentiation.

For the next result, we use the fact that $(\mathbb{N}, \leq)$ is a well-ordered set, i.e., every non-empty subset of $\mathbb{N}$ has a least element. Prove using induction.

Theorem 1.7. *There is no $x \in \mathbb{Q}$ such that*

$$x^2 = 2.$$

Proof. Suppose there is such an x. Since $(-x)^2 = x^2$ (field properties), we may assume that $x > 0$. Thus, $x = p/q$ for some $p, q \in \mathbb{N}$. Thus, the set

$$X = \{q \in \mathbb{N}^* : x = p/q \text{ for some } p \in \mathbb{N}\}$$

is non-empty. By the well-ordering principle, X admits a least element, say q_0. Let $p_0 \in \mathbb{N}$ be such that $x = p_0/q_0$. Since x must be in $(1,2)$,

$$p_0 > q_0 \quad \text{and} \quad q_0 > p_0 - q_0.$$

Now,

$$\frac{2q_0-p_0}{p_0-q_0}=\frac{2-x}{x-1}=\frac{(2-x)(x+1)}{x^2-1}=\frac{2-x^2+x}{1}=x.$$

This contradicts the minimality of q_0. □

Theorem 1.8. *Let*

$$\begin{aligned} A &= \{x\in\mathbb{Q}: x^2<2\} \\ B &= \{x\in\mathbb{Q}: x^2>2\}. \end{aligned}$$

For any $a\in A$, there is a $c\in A$ such that $a<c$. Similarly, for any $b\in B$, there is a $d\in B$ such that $d<b$.

Proof. We prove the first statement, and leave the second as exercise. Let $a\in A$. If $a\le 0$, then $c=0$ works. So, we may assume that $a>0$. Let

$$c=a+\frac{2-a^2}{2+a}=\frac{2a+2}{2+a}.$$

Then, clearly $c>a$, and $c^2-2=\frac{2(a^2-2)}{(a+2)^2}<0$. The idea is that we want to create a number between a and “$\sqrt{2}$". Note that

$$\text{“}\sqrt{2}\text{"}=a+(\sqrt{2}-a)\frac{\sqrt{2}+a}{\sqrt{2}+a}>a+\frac{2-a^2}{2+a}$$

which is a rational number. □

Recap from 101 Lecture 6 definitions of bounded sets, upper & lower bounds, the greatest lower bound (infimum) and the least upper bound (supremum). The above theorem implies that $\mathbb{Q}$ does not have the *least upper bound property*, i.e., there is a set $S\subset\mathbb{Q}$ that is bounded from above, but does not admit a least upper bound in $\mathbb{Q}$.

1.5. **Ordered fields with the least upper bound property.** We tackle existence of such fields later. We first discuss some important properties.

Theorem 1.9. *Let F be an ordered field ~~with the l.u.b. property~~. Then, F “contains" $\mathbb{Q}$ as a subfield, i.e., there is an injective map $f:\mathbb{Q}\to F$ that respects addition, multiplication and order.*

Proof. Let $f:\mathbb{Z}\mapsto F$ be given by

$$f(n)=\begin{cases} 0_F, & \text{if } n=0,\\ 1_F, & \text{if } n=1,\\ n\cdot 1_F=1_F+\cdots+1_F(n\text{ times}), & \text{if } n>1,\\ n\cdot 1_F=-1_F+\cdots+(-1_F)(-n\text{ times}), & \text{if } n<0. \end{cases}$$

Then, f is an injective map that respects addition, multiplication & order. We establish injectivity (and leave the rest as exercise). Say $f(m) = f(n)$ for some $m < n$. Then, $0_F = f(n-m) = (n-m)\cdot 1_F > 0$, where the last inequality holds because

- (*) $0_F < 1_F$,
- (*) $0_F + 1_F < 1_F + 1_F$,
- (*) induction.

This is a contradiction. Now, extend f to $\mathbb{Q}$ by setting

$$f(a/b) = f(a)\frac{1}{f(b)}, \quad a \in \mathbb{Z}, b \in \mathbb{Z}^*.$$

This is a well-defined ordered field isomorphism. □

For simplicity, we identify z and $f(z)$, and write $\mathbb{Q} \subset F$. Note that, for any $n \in \mathbb{N}$ and $x \in F$,

$$nx = x + \cdots + x \ (n \text{ times}). \tag{1.1}$$

This is because $n = 1 + \cdots 1$ (n times), by the identification done above.

END OF LECTURE 3