MATH 117 FALL 2014 LECTURE 3 (SEPT. 5, 2014)

- How detailed should your answers to Homework 1 be:

  For example, to prove that the product of two odd numbers is still odd, you should write something like:

  > Recall that a natural number a is odd if and only if $a = 2\,k - 1$ for some natural number k.
  >
  > Denote by a, b the two odd numbers. Then there are natural numbers k, l such that $a = 2\,k - 1, b = 2\,l - 1$. This gives
  >
  > $$a\,b = (2\,k - 1)\,(2\,l - 1) = 4\,k\,l - 2\,k - 2\,l + 1 = 2\,(2\,k\,l - k - l + 1) - 1. \tag{1}$$
  >
  > If we denote $m := 2\,k\,l - k - l + 1$ then we have $a\,b = 2\,m - 1$. The only thing left to show is $m \geqslant 1$ and is thus a natural number. We notice
  >
  > $$2\,k\,l - k - l + 1 = k\,l + (k - 1)\,(l - 1) \geqslant k\,l \geqslant 1. \tag{2}$$
  >
  > Therefore $m \geqslant 1$ is a natural number and $a\,b$ must be odd.

- Last bit of number theory.
  - Recall the Fundamental Theorem of Arithmetic:

    > Every natural number greater than 1 either is prime or is a product of primes. Furthermore, this factorization is unique: the order of the primes is arbitrary, but the primes themselves are not.

  - Now we prove an immediate but important consequence:

    COROLLARY 1. *Let p be prime and let $a, b \in \mathbb{N}$ (meaning: a, b are members of the set/collection $\mathbb{N}$, in other words a, b are natural numbers). If $p|\,(a\,b)$ then either $p|\,a$ or $p|\,b$.*

    Proof. Let $a = p_1 \cdots p_r$; $b = q_1 \cdots q_s$ be the unique prime factorizations of a, b respectively. Then we have

    $$a\,b = p_1 \cdots p_r\,q_1 \cdots q_s. \tag{3}$$

    By the Fundamental Theorem of Arithmetic, this is the unique factorization of $a\,b$. Since $p|\,(a\,b)$, p equals one of $p_1, \ldots, p_r, q_1, \ldots, q_s$. Now if $p = p_i$ for some $i \in \{1, \ldots, r\}$, we have $p|\,a$. If not then necessarily $p = q_j$ for some $j \in \{1, \ldots, s\}$ which leads to $p|\,b$. ☐

    Remark 2. Note that p being prime is crucial here.

    Exercise 1. Let $a, b, c \in \mathbb{N}$ and assume $c|\,(a\,b)$. Does it follow that $c|\,a$ or $c|\,b$? Justify.

    Note. "Justify" means you should prove your claim.

- $\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q}$.
  - The generalizations come from algebra.[1]
  - Solving $x + a = b$ for all $a, b \in \mathbb{N}$ leads to $\mathbb{Z}$.

    Example 3. Prove $(-1) \cdot (-1) = 1$.

---

1. The word "algebra" comes from the book *Hidab al-jabr wal-muqubala* written in 825AD by al-Khwarizmi, whose name becomes "algorithm". The title means "Science of restoration and confrontation" where "restoration" is $x - 2 = 7 \Longrightarrow x = 9$ (restored!) and "confrontation" is $x + 3 = 10 \Longrightarrow x + 3 = 3 + 7 \Longrightarrow x = 7$ where the two 3's confront each other and cancel.

Proof. We have

$$(-1)\cdot 1+1\cdot 1=(-1+1)\cdot 1=0\cdot 1=0 \tag{4}$$

and on the other hand

$$(-1)\cdot 1+(-1)\cdot(-1)=(-1)\cdot(1+(-1))=(-1)\cdot 0=0. \tag{5}$$

Therefore

$$(-1)\cdot 1+1\cdot 1=(-1)\cdot 1+(-1)\cdot(-1) \tag{6}$$

which (through confrontation!) gives $1\cdot 1=(-1)\cdot(-1)$ and the proof ends. □

Remark 4. It is important to notice that, mysteriously, once we extend $\mathbb{N}$ to $\mathbb{Z}$, no more extension is needed to be able to solve $x+a=b$ for all $a,b\in\mathbb{Z}$ (not only in $\mathbb{N}$!)

- Solving $x\cdot a=b$ for all $a,b\in\mathbb{Z}$ leads to $\mathbb{Q}$.
  - Thus we have

    $$\mathbb{Q}=\left\{\frac{p}{q}|\, p,q\in\mathbb{Z}, q>0, (p,q)=1\right\} \tag{7}$$

    that is

    > any rational number can be written uniquely as $\frac{p}{q}$ where p, $q\in\mathbb{Z}$, $q>0$, and the greatest common divisor of (p,q) is 1.

    The requirement $q>0$ is necessary since otherwise we would have two representations for one rational number, for example $\frac{2}{5}=\frac{-2}{-5}$.
  - We can define "order" on $\mathbb{Q}$.[2] Let $a=\frac{p_1}{q_1}, b=\frac{p_2}{q_2}\in\mathbb{Q}$, where the representations $\frac{p_1}{q_1},\frac{p_2}{q_2}$ satisfy the requirements in (7). Then we say
    - $a=b$ if and only if $p_1\, q_2=p_2\, q_1$;
    - $a<b$ if and only if $p_1\, q_2<p_2\, q_1$;
    - $a>b$ if and only if $b<a$.

    Exercise 2. Let $a,b\in\mathbb{Q}$. Prove that exactly one of the following holds: $a=b, a<b, a>b$.

    Exercise 3. In this exercise we prove that this order on $\mathbb{Q}$ is consistent with the order on $\mathbb{Z}$. Let $a,b\in\mathbb{Z}$. Then $a,b\in\mathbb{Q}$. Prove that $a<b$ as integers if and only if $a<b$ as rationals (that is if $a<b$ as integers then $a<b$ as rationals, and if $a<b$ as rationals then $a<b$ as integers.)

    Exercise 4. Let $a,b,c\in\mathbb{Q}$. Prove that $a<b, b<c$ then $a<c$.
  - Operations on $\mathbb{Q}$.

    NOTATION. *":=" means "defined as".*

    $$\frac{p_1}{q_1}+\frac{p_2}{q_2}:=\frac{p_1\, q_2+p_2\, q_1}{q_1\, q_2}. \tag{8}$$

    $$\frac{p_1}{q_1}-\frac{p_2}{q_2}:=\frac{p_1\, q_2-p_2\, q_1}{q_1\, q_2} \tag{9}$$

    $$\frac{p_1}{q_1}\cdot\frac{p_2}{q_2}:=\frac{p_1\, p_2}{q_1\, q_2}. \tag{10}$$

2. Note that here we have obtained $\mathbb{Q}$ from $\mathbb{Z}$, therefore we should define the order on $\mathbb{Q}$ through operations in $\mathbb{Z}$. As of now we haven't defined the set of real numbers $\mathbb{R}$ yet, and therefore there is no natural "order" that $\mathbb{Q}$ could inherit.

Exercise 5. Let $a, b \in \mathbb{Q}$. Prove that $a < b$ if and only if $a - b < 0$. Make sure you realize that this indeed needs to be proved.[3]

Remark 5. What is wrong with defining

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 + p_2}{q_1 + q_2}? \tag{11}$$

The answer is nothing is wrong, except that the "numbers" $\frac{p}{q}$ with this addition rule do not behave like everyday numbers anymore. Indeed, if we take away – and put (), (11) becomes the perfect vector addition rule:

$$\begin{pmatrix} p_1 \\ q_1 \end{pmatrix} + \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} = \begin{pmatrix} p_1 + p_2 \\ q_1 + q_2 \end{pmatrix}. \tag{12}$$

Remark 6. An article that may be too early to mention now is *Successive generalizations in the theory of numbers* by Eric Temple Bell in The American Mathematical Monthly, Vol. 34, no. 2, Feburary 1927, pp. 55-75. You need to know abstract algebra to understand it, but on the other hand it could help you understand why people bother to define things like ideals.

- Properties of $\mathbb{Q}$.
  - The most important property of $\mathbb{Q}$ is that it is dense:

    Let a, $b \in \mathbb{Q}$, $a \neq b$. Then there is $c \in \mathbb{Q}$ lying in between a and b.

Proof. Let $a, b \in \mathbb{Q}$, $a \neq b$. Then either $a < b$ or $a > b$. We prove the former case and leave the latter as exercise. Let $a = \frac{p_1}{q_1}$, $b = \frac{p_2}{q_2}$. Then $a < b$ means $p_1\, q_2 < p_2\, q_1$.

Now take $c = \frac{a+b}{2} = \frac{p_1\, q_2 + p_2\, q_1}{2\, q_1\, q_2}$. We try to prove $a < c < b$. First we prove $a < c$. By definition all we need to prove is

$$2\, p_1\, q_1\, q_2 < p_1\, q_1\, q_2 + p_2\, q_1^2. \tag{13}$$

Now as $a < b$ we have $p_1 q_2 < p_2\, q_1$. As $q_1 > 0$ we can multiply both sides by q_1 to obtain

$$p_1\, q_1\, q_2 < p_2\, q_1^2. \tag{14}$$

Now adding $p_1\, q_1\, q_2$ to both sides we obtain (13) and finishes the proof of $a < c$.

Exercise 6. Prove $c < b$. □

Exercise 7. Prove the case $a > b$.

3. Because our definitions of $a < b$ and $a - b$ are independently given.