# Notes for 8th Jan (Tuesday)

## 1 The road so far...

1. Defined partial, total, and well orders. Stated the well ordering principle and Zorn's lemma.
2. Defined cardinality and proved that $|X| < |P(X)|$.

## 2 Cardinality

This means that $\mathbb{N}$ has strictly "smaller" than its power set. A natural question is :

*The continuum hypothesis* : Is there any set in between the naturals and its power set ? That is, one that admits an injection from the naturals, but not a surjection and does not surject to the power set of the naturals ?

Paul Cohen won a fields medal for proving that this question can neither be proven or disproven in ZFC.

## 3 Integers

So far we have addition, and a "cancellation" property but we do not have numbers to add to 1 to get 0, i.e., you can borrow money but not lend it. So we want to define integers as follows :
An integer is a pair of natural numbers $(a, b)$ written as $a - b$.
But let's be more precise. First, we need to know what an equivalence relation on a set $A$ is : It is a subset $R$ in $A \times A$ such that

1. Reflexivity : $(a, a) \in R$
2. Symmetry : $(a, b) \in R \Rightarrow (b, a) \in R$
3. Transitivity : $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$.

If $(a, b) \in R$ we write $a \equiv b$. An equivalence relation partitions a set into equivalence classes, i.e., subsets $E$ such that they are disjoint and their union is $A$. Each $E$ consists of elements equivalent to one another.
Define an equivalence relation on pairs of natural numbers saying $(a, b) \equiv (c, d)$ if

$a + d = b + c$. This splits the pairs into equivalence classes. The set of these equivalence classes (which is a subset of $\mathbb{N} \times \mathbb{N}$) is called $\mathbb{Z}$ (integers). Every integer is written as $a - b$ instead of $(a, b)$ where $(a, b)$ is any representative of the equivalence class.

Addition : $(a - b) + (c - d)$ is defined to be $(a + c) - (b + d)$.

Multiplication : $(a - b) \times (c - d) = (ac + bd) - (ad + bc)$.

We need to show that these are well-defined, i.e. if we replace $a - b$ with another representative $\alpha - \beta$ such that $a + \beta = b + \alpha$, then we should get the same integers in the above definitions (and likewise for $c - d$ replaced with $\gamma - \delta$). Let's verify that addition is well-defined. Multiplication is similar.

We claim that $(\alpha + \gamma) - (\beta + \delta) \equiv (a + c) - (b + d)$. Indeed,

$$(\alpha + \gamma) + (b + d) = b + \alpha + d + \gamma = a + \beta + c + \delta = (a + c) + (\beta + \delta)$$

Now define a map $\iota : \mathbb{N} \to \mathbb{Z}$ as $\iota(n) = n - 0$. This is a bijection that respects addition and multiplication. (Exercise.) Thus the natural numbers "sit" inside the integers.

The negation of an integer $a - -b$ is defined as $-(a - b) = b - a$. One can prove the trichotomy law, i.e., every integer is either 0, a positive natural number, or $-n$ where $n$ is a positive natural number.

Now we may state and prove that integers satisfy all the nice properties that we are used to :

1. $x + y = y + x$
2. $x + 0 = 0 + x = x$
3. $x + (-x) = (-x) + x = 0$
4. $(x + y) + z = x + (y + z)$
5. $x \times y = y \times x$
6. $x \times (y + z) = x \times y + x \times z$
7. $(x \times y) \times z = x \times (y \times z)$
8. $x \times 1 = 1 \times x = x$

Objects that obey the above laws are called commutative rings. (So the properties above say that $\mathbb{Z}$ is a commutative ring.) We can define subtraction of two integers $x - y$ as $x + (-y)$. (Check that this is well-defined.)

Some other properties are

1. No zero divisors (i.e. $ab = 0$ if and only if $a = 0$ or $b = 0$).

2. Cancellation law : If $ac = bc$ and $c \neq 0$ then $a = b$.

Ordering : $n \geq m$ if $n = m + a$ for some natural number $a$. If $n \geq m$ and $n \neq m$, we say $n > m$. With this definition, it is easy to prove the usual properties of order :

1. $a > b$ if and only if $a - b$ is a positive natural number.
2. If $a > b$, then $a + c > b + c$.
3. If $a > b$, and $c > 0$ then $ac > bc$.
4. If $a > b$ then $-a < -b$.
5. If $a > b$ and $b > c$, then $a > c$.
6. Either $a = b$ xor $a > b$ xor $a < b$.

Finally, the set of integers has the same cardinality as that of natural numbers. Indeed, a bijection is $f(2n - 1) = n, f(2n) = -n$.

# 4 Rational numbers

We do not know how to divide a banana into two equal parts. So now we define the rational numbers formally -

The set $\mathbb{Q}$ of rational numbers is the set of equivalence classes of pairs of integers $(a, b)$ (written as $a/b$) where $b \neq 0$ such that $a/b \equiv c/d \Leftrightarrow ad = bc$.

One can prove that rationals are countable (by first proving that $\mathbb{N} \times \mathbb{N}$ is so).

We may define negation as $-p/q = (-p)/q$, addition as $p/q + r/s = (ps + qr)/qs$ and multiplication as $p/q \times r/s = (pr)/(qs)$.

You can make $\mathbb{Z}$ sit bijectively in $\mathbb{Q}$ whilst respecting addition, multiplication (and ordering as we shall see) via : $\iota(n) = n/1$.

Define the reciprocal $x^{-1}$ of a non-zero rational (i.e. when $x \neq 0/1$) as follows : If $x = p/q$, then $x^{-1} = q/p$.

Properties of rationals :

1. $x + y = y + x$
2. $x + (y + z) = (x + y) + z$
3. $x + 0 = 0 + x = x$
4. $x + (-x) = (-x) + x = 0$
5. $xy = yx$

6. $(xy)z = x(yz)$

7. $(x+y)z = xz + yz$

8. $x.1 = 1.x = x$

and finally,
$x.x^{-1} = x^{-1}.x = 1$ if $x \neq 0$.
Objects satisfying the above properties are called "Fields". ($\mathbb{Q}$ is a field.)
We define *division* of rationals $x$ and $y \neq 0$ as $x \div y = xy^{-1}$.
We say that $x$ is positive if $x = p/q$ for two positive integers $p$ and $q \neq 0$. $x$ is negative if $x = -y$ for some positive rational $y$. Also, $x$ is said to be $\geq y$ if $x = y + z$ for some positive rational and $x > y$ if $x \geq y$ and $x \neq y$. Likewise for $\leq$.
We have the following properties of ordering :

1. $x = 0$ xor $x$ is positive xor $x$ is negative.

2. For every $x$ and $y$, $x = y$ xor $x > y$ xor $x < y$.

3. If $x < y$ then $y > x$.

4. $x < y, y < z \Rightarrow x < z$.

5. $x < y \Rightarrow x + z < y + z$.

6. If $x < y$ and $z$ is positive, then, $xz < yz$.

## 4.1 A digression - Pythagorean triples

Suppose we want to find integers $a, b, c$ such that $a^2 + b^2 = c^2$. Then this is equivalent to solving $x^2 + y^2 = 1$ for rational $(x, y)$. A nice way to do this is using geometry. We just want to find rational points on the unit circle $S^1$. One such point is $(1, 0)$. All the other points are obtained using the following lemma.

**Lemma 4.1.** *$(x, y) \in S^1$ is rational if and only if the line joining it to $(1, 0)$ has rational slope.*

*Proof.* Indeed, if $y = m(x-1)$, then of course $m$ is rational if $x$ and $y$ are. Conversely, $x^2 + m^2(x-1)^2 = 1 \Rightarrow x^2(1+m^2) - 2m^2x + m^2 - 1 = 0$. Hence $x = \frac{m^2-1}{m^2+1}$ and $y = \frac{\pm 2m}{m^2+1}$ implying that $(x, y)$ is rational. □

The above proof also produces a formula for all Pythagorean triples. This sort of reasoning can be extended to more number of variables. Unfortunately, this is where the fun stops. As we all know, $x^n + y^n = z^n$ does not have integral solutions when $n \geq 3$. This way of using geometry in number theory is vastly exploited in the subject of arithmetic geometry (which was used along with other techniques to prove Fermat's last theorem by Wiles).