LECTURE 3

We continue deriving some simple consequences of Axiom I (the algebraic axiom). We observe that

8. if $x, y \in \mathbb{R}$ and $xy = 0$ then $x = 0$ or $y = 0$. We prove this as follows. Suppose $xy = 0$. If $x \neq 0$ then

$$\begin{aligned} & 0 = x^{-1}0 \quad \text{(by 6. from last time)} \\ \Longrightarrow\ & 0 = x^{-1}(xy) \\ \Longrightarrow\ & 0 = (x^{-1}x)y \quad \text{(by (f))} \\ \Longrightarrow\ & 0 = 1y \quad \text{(by (h))} \\ \Longrightarrow\ & 0 = y \quad \text{(by (g))} \end{aligned}$$

Therefore $x = 0$ or $y = 0$.

9. We introduce shorthand such as

- $x + y + z = (x + y) + z, \ldots$
- $2 = 1 + 1$, $3 = 1 + 1 + 1$, $\ldots$,
- $x^2 = x \cdot x$, $\ldots$,
- $x - y = x + (-y)$,

and we prove identities such as

$$(x + y)^2 = x^2 + 2xy + y^2.$$

Note that there is nothing in the rules that we wrote down that prevents $2 = 0$!

A set F satisfying all of the requirements of Axiom I (with $\mathbb{R}$ replaced by F) is known in mathematics as a *field*. There are lots of examples of fields, for instance $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ as well as other examples such as

$$\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \mid \ a, b \in \mathbb{Q} \,\}$$

with addition and multiplication defined by

$$\begin{aligned} (a + b\sqrt{2}) + (a' + b'\sqrt{2}) &= (a + a') + (b + b')\sqrt{2} \\ (a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) &= (aa' + 2bb') + (ab' + a'b)\sqrt{2} \end{aligned}$$

and where we define $a + b\sqrt{2} = a' + b'\sqrt{2}$ if and only if $a = a'$ and $b = b'$. It is not hard to check that all of the rules (a)–(i) are satisfied in this case (probably the trickiest thing is to check that if $a + b\sqrt{2} \neq 0$ then $a + b\sqrt{2}$ has a multiplicative inverse).

Here is a question you might ask: what is the smallest possible field? Well, it would have to contain an element 0, and a different element 1. Is there a field with just these two elements? If there was, then the rule for multiplication would have to be

$$\begin{aligned} & 0 \cdot 0 = 0 \cdot 0 = 0 \\ & 0 \cdot 1 = 1 \cdot 0 = 0 \\ & 1 \cdot 1 = 1 \end{aligned}$$

We would also have to have $0 + 0 = 0$ and $0 + 1 = 1 = 1 + 0$. What about $1 + 1$? This must equal 0, if 1 is to have an additive inverse. You can check that the set $\{0, 1\}$ with these rules for multiplication and addition is a field; it is denoted $\mathbb{F}_2$.

We now want to impose an axiom on $\mathbb{R}$ which lets us talk about inequalities.

Axiom II (the order axiom) there is a relation $<$ on $\mathbb{R}$ defined in such a way that $a < b \iff 0 < b - a$ and which satisfies the following rules:

(a) for all $x \in \mathbb{R}$ exactly one of the following statements is true:

0¡x, x =0, or 0 ¡ -x.

(b) if $0 < x, 0 < y$ then $0 < x + y$.

(c) if $0 < x, 0 < y$ then $0 < xy$.

Thus this axiom specifies a subset of *positive elements* of $\mathbb{R}$ and prescribes some rules which state that this subset of positive elements is preserved under addition and multiplication.

Again, we make some observations.

1. To begin with we observe that $0 < 1$. We have assumed that $0 \neq 1$; therefore, by (a) above, either $0 < 1$ or $0 < -1$. If it is not true that $0 < 1$ then the only possibility is that $0 < -1$. If this was the case then by (c) we would have $0 < (-1)(-1) = -(-1) = 1$. But then $0 < -1$ and $0 < 1$, a contradiction. Therefore we must have $0 < 1$.

2. We define $x > y$ if $y < x$. We define $x \leq y$ if $x = y$ or $x < y$. We define $x \geq y$ if $x = y$ or $x > y$.

3. By 1. above we have $2 = 1 + 1 > 0$, $3 > 0$, ...etc. In particular $2 \neq 0$.

4. If $x < y$ and $y < z$ then $x < z$. To see this we observe that $0 < y - x$ and $0 < z - y$; hence by (b) $0 < (y - x) + (z - y) = z - x$. Therefore $x < z$.

5. If $x < y$ then $x + z < y + z$ for any $z \in \mathbb{R}$ since $0 < y - x = (y + z) - (x + z)$.

6. If $x < y$ and $z > 0$ then $xz < yz$. To see this, by (c) we have $(y - x)z > 0$, i.e. $yz - xz > 0$ and hence $xz < yz$.

7. We define the following distinguished subsets of $\mathbb{R}$ called *intervals*. If $a < b$ then

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R} \mid \ a < x < b\} \\
(a, b] &= \{x \in \mathbb{R} \mid \ a < x \leq b\} \\
[a, b) &= \{x \in \mathbb{R} \mid \ a \leq x < b\} \\
[a, b] &= \{x \in \mathbb{R} \mid \ a \leq x \leq b\}.
\end{aligned}$$

If $a \in \mathbb{R}$ then we define

$$\begin{aligned}
&(a, \infty) = \{x \in \mathbb{R} \mid \ x > a\} \\
&[a, \infty) = \{x \in \mathbb{R} \mid \ x \geq a\} \\
&(-\infty, a) = \{x \in \mathbb{R} \mid \ x < a\} \\
&(-\infty, a] = \{x \in \mathbb{R} \mid \ x \leq a\} \\
&(-\infty, \infty) = \mathbb{R}.
\end{aligned}$$

8. We've observed above that if n is a natural number then we can define a real number

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} \in \mathbb{R}.$$

Momentarily, let us distinguish this real number n from the natural number n by writing $f(n)$ for the real number n. It should be clear that if m is another natural number then $f(m+n) = f(m) + f(n)$. Thus we have a function $f\colon \mathbb{N} \to \mathbb{R}$ which *preserves addition*. We can enlarge the domain of the function f to the set of integers $\mathbb{Z}$ by defining $f(-n) = -f(n)$ if n is a natural number, and by defining $f(0) = 0$. Again, the new function $f\colon \mathbb{Z} \to \mathbb{R}$ preserves addition and additive identities (if you have taken Algebra II, then you would recognize such a function as being a *homomorphism* of additive groups). The function $f\colon \mathbb{Z} \to \mathbb{R}$ is injective, i.e. $f(m) = f(n) \implies m = n$. The reason for this is that if $n > 0$ in $\mathbb{Z}$ then $f(n) > 0$ in $\mathbb{R}$ while if $n < 0$ in $\mathbb{Z}$ then $f(n) < 0$ in $\mathbb{R}$; it follows from this that f is injective (again, this should be clear if you have done Algebra II). It is possible to enlarge the domain of the function f again, this time extending $\mathbb{Z}$ to it's 'field of fractions' $\mathbb{Q}$; one can show that the new function $f\colon \mathbb{Q} \to \mathbb{R}$ is injective, and satisfies

$$f(q_1 + q_2) = f(q_1) + f(q_2), \quad f(q_1 \cdot q_2) = f(q_1) \cdot f(q_2), \quad f(0) = 0, \quad f(1) = 1.$$

What this means is that you can identify $\mathbb{Q}$ with it's image $f(\mathbb{Q})$ inside $\mathbb{R}$; we think of this as the statement that $\mathbb{R}$ 'contains a copy of $\mathbb{Q}$' and that the operations of addition and multiplication on $\mathbb{R}$ restrict to the usual operations of addition and multiplication on $\mathbb{Q}$.

A set F which satisfies Axioms I and II (with $\mathbb{R}$ replaced by F) is known in mathematics as an *ordered field*. $\mathbb{Q}$ and $\mathbb{R}$ are both ordered fields. The smallest possible field $\mathbb{F}_2$ is not an ordered field. The complex numbers $\mathbb{C}$ do not form an ordered field. Suppose they did — suppose that $<$ was an order relation on $\mathbb{C}$. Then either $i > 0$ or $-i > 0$. If $i > 0$ then $-1 = i^2 > 0$, which contradicts our discovery in 1. above (that same argument applies to any ordered field F). If $-i > 0$ then $-1 = (-i)(-i) > 0$ which again contradicts 1. above. Therefore such an order on $\mathbb{C}$ cannot exist.

Before we finish this discussion of order, we need to introduce one more concept, that of absolute value. If $x \in \mathbb{R}$, then we define a number $|x| \in \mathbb{R}$ (called the *absolute value* of x) by

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } -x > 0. \end{cases}$$

There is an extremely important inequality involving the absolute value that we will make continual use of throughout the course. This is the *triangle inequality* which says that

$$|x + y| \leq |x| + |y|$$

for all real numbers x and y.

The crucial axiom

We've observed that the set of rational numbers has 'gaps' — for instance $\sqrt{2}$ is not a rational number. One manifestation of these gaps is that the rational numbers can be partitioned into two sets around such a gap, e.g.

$$\mathbb{Q} = \{\, x \in \mathbb{Q} \mid \ x^2 < 2 \text{ or } x < 0 \,\} \cup \{\, x \in \mathbb{Q} \mid \ x^2 > 2 \text{ and } x \geq 0 \,\}.$$

In $\mathbb{R}$ these gaps should be filled. The following axiom is one way of making this intuition precise.

Axiom III′: if A and B are subsets of $\mathbb{R}$ such that

(a) $A \neq \emptyset, B \neq \emptyset$
(b) $A \cup B = \mathbb{R}$
(c) for all $a \in A$ and for all $b \in B$ we have $a < b$,

then there exists $c \in \mathbb{R}$ such that either

$$A = (-\infty, c), B = [c, \infty) \quad \text{or} \quad A = (-\infty, c], B = (c, \infty).$$

We could state Axiom III$'$ more generally for an ordered field F: this would be the statement that for all non-empty subsets A and B of F such that $A \cup B = F$ and such that for all $a \in A$ and for all $b \in B$ the inequality $a < b$ holds, there exists $c \in F$ such that either $A = (-\infty, c), B = [c, \infty)$ or $A = (-\infty, c], B = (c, \infty)$.

Axiom III$'$ is not satisfied for the ordered field $\mathbb{Q}$. What this means is that there are some non-empty subsets A and B of $\mathbb{Q}$ such that $A \cup B = \mathbb{Q}$ and $a < b$ for all $a \in A$ and for all $b \in B$, but there is no rational number c such that $A = (-\infty, c), B = [c, \infty)$ or $A = (-\infty, c], B = (c, \infty)$. An example of such a pair of sets A and B is

$$A = \{\, x \in \mathbb{Q} \mid \ x^2 < 2 \text{ or } x < 0 \,\}, B = \{\, x \in \mathbb{Q} \mid \ x^2 > 2 \text{ and } x \geq 0 \,\}.$$

This is in fact not so obvious. However, what one can prove is that A has no largest element (and hence A cannot equal $(-\infty, c]$ for any rational number c) and that B has no smallest element (and hence B cannot equal $[c, \infty)$ for any rational number c).

If $q \in A$ we will show that there is a positive rational number r with $0 < r < 1$ such that $q + r \in A$. It follows that A cannot have a largest element. We estimate how big r should be in order to have $(q + r)^2 < 2$:

$$(q + r)^2 = q^2 + 2qr + r^2 < q^2 + (2q + 1)r < 2 \iff r < \frac{2 - q^2}{2q + 1}.$$

Therefore we may take $r = (2 - q^2)/(4q + 2)$. The proof that B has no smallest element is similar.