LECTURE 2

As mentioned last time there are four main methods of proof that we shall use in this course. Last time we mentioned direct proof and proof by contradiction. If you are trying to prove a statement of the form 'Statement $P(n)$ is true for all natural numbers n', then there is another method of proof that is sometimes useful. This is the method of proof by *Principle of Mathematical Induction*. The strategy that is employed here is as follows:

1. Prove the initial case when $n = 1$, i.e. prove the statement $P(1)$.

2. Assume that $k > 1$ is a natural number and that $P(k)$ is true. Under this assumption prove that $P(k + 1)$ is true.

You then conclude that the statement $P(n)$ is true by the Principle of Mathematical Induction. It turns out that the Principle of Mathematical Induction is in fact equivalent to a statement about the set $\mathbb{N}$ of natural numbers. This statement is the following

Well Ordering Principle: if S is a non-empty subset of $\mathbb{N}$ then S has a least element, i.e. a smallest element.

This is a very plausible statement about $\mathbb{N}$ — after reflecting on it for a while, you would probably accept it without hesitation. On the other hand, the Well Ordering Principle is either an axiom that you impose on the natural numbers (and as a consequence you can *prove* the Principle of Mathematical Induction), or you *accept* the Principle of Mathematical Induction and use it to prove the Well Ordering Principle. The choice is more or less up to the tastes of the individual.

Another useful strategy is proof of the *contrapositive statement*. This applies in the following situation: sometimes you want to prove a statement of the form $A \implies B$ (such a statement is called a *conditional statement*). The strategy is that you prove instead the statement (not B) $\implies$ (not A). This is the *contrapositive* of the statement $A \implies B$. The point is that the original statement and its contrapositive are *logically equivalent* — that means they're either both true or they're both false.

It's important not to confuse the contrapositive of $A \implies B$ with the *converse* of $A \implies B$. The converse of $A \implies B$ is the statement $B \implies A$; this is usually different from the statement (not B) $\implies$ (not A).

For example, consider the statement 'Let $n \in \mathbb{Z}$. If $n^2 - 3n + 3$ is even, then n is odd'. The contrapositive statement is the statement

$$\text{Let } n \in \mathbb{Z}. \text{ If } n \text{ is even, then } n^2 - 3n + 3 \text{ is odd.}$$

This is easier to prove than the original statement. Try it and see. We're now ready to start discussing the real numbers in a little more detail.

1. The Axioms of Real Analysis

We accept that we can't give precise values to expressions like $\sqrt{2}+\pi$ in terms of infinite decimals. In our experience so far with calculus, we have been perfectly content to leave an expression like $\sqrt{2} + \pi$ as an answer, say as the answer to the problem of calculating an integral. What we want most from real numbers is to manipulate them algebraically as we have been doing, for instance manipulations such as

- $(x+y)^2 = x^2 + 2xy + y^2$,
- $(x^2y^{-1})^3 = x^6y^{-3}$,
- $\sqrt{7+4\sqrt{3}} = 2+\sqrt{3}$.

The last example comes about because $7+4\sqrt{3} = (2^2) + (\sqrt{3})^2 + 4\sqrt{3} = (2+\sqrt{3})^2$. Hence $\sqrt{7+4\sqrt{3}} = |2+\sqrt{3}| = 2+\sqrt{3}$. So we want to be able to do things like take square roots of (non-negative) real numbers and take absolute values. Another important aspect of real numbers is that we can *compare* them via inequalities — there is a notion of *order* on the real numbers which lets us say when a real number x is greater than or equal to a real number y.

Another important feature of real numbers is that we can compare them — in other words we can make sense of what it means for a real number x to be less than a real number y, i.e. $x < y$. We will make constant use of inequalities throughout this course — be prepared! Whatever the real numbers are, we would like to be able to argue as in the following example: prove that $\sqrt{2} + \pi < 2 + \sqrt{\pi}$ (note that implicit in this is the assertion that we can take square roots of non-negative real numbers, and there is a positive real number π; convincing ourselves that these assertions are true is some way off). We have $1 < \sqrt{2}$, $3 < \pi$ and $\sqrt{\pi} < 2$; therefore

$$2 + \sqrt{\pi} < 2 + 2 = 1 + 3 < \sqrt{2} + \pi.$$

The fact that validates this is that if $x < y$ and $z < w$ then $z + z < y + w$; we will certainly want this fact to be true for the real numbers.

Therefore, based on these examples, we want to be able to add, subtract, multiply and divide real numbers, and we also want a notion of $<$. Motivated by this, we introduce our first axiom, which specifies the algebraic structure that the real numbers should possess.

Axiom I (the algebraic axiom): there is a set $\mathbb{R}$, whose elements are called *real numbers*, equipped with binary operations $+, \cdot$ so that for every pair x, y of real numbers there is a real number $x + y$ (the *sum*) and a real number $x \cdot y$ (*the product*). There are real numbers 0, 1 and $0 \neq 1$. The following rules are satisfied:

(a) $x + y = y + x \ \forall\ x, y \in \mathbb{R}$ (*commutativity* of addition).
(b) $x + (y + z) = (x + y) + z \ \forall\ x, y, z \in \mathbb{R}$ (*associativity* of addition).
(c) $x + 0 = x + 0 = x \ \forall\ x \in \mathbb{R}$ (additive *identities*).
(d) if $x \in \mathbb{R}$ then $\exists\ -x \in \mathbb{R}$ such that $x + (-x) = 0$ (additive *inverses*).
(e) $x \cdot y = y \cdot x \ \forall\ x, y \in \mathbb{R}$ (*commutativity* of multiplication).
(f) $x \cdot (y \cdot z) = (x \cdot y) \cdot z \ \forall\ x, y, z \in \mathbb{R}$ (*associativity* of multiplication).
(g) $x \cdot 1 = x \ \forall\ x \in \mathbb{R}$ (multiplicative *identities*).
(h) if $x \in \mathbb{R}$, $x \neq 0$, then $\exists\ x^{-1} \in \mathbb{R}$ such that $x \cdot x^{-1} = 1$ (multiplicative *inverses*).
(i) $x \cdot (y + z) = x \cdot y + x \cdot z \ \forall\ x, y, z \in \mathbb{R}$ (*distributivity*).

Notice that we have started to use the *quantifiers* $\forall$ and $\exists$ from symbolic logic; remember that $\forall$ means 'for all' and $\exists$ means 'there exists'.

Let's now discuss some questions that come to mind about these axioms and also let's make some simple deductions from these axioms.

1. There can be only one number 0 which satisfies rule (c): if there was another number $0'$, which also satisfied (c) (i.e. $x + 0' = x = 0' + x$ for all $x \in \mathbb{R}$) then we would have $0 = 0 + 0'$ (since $0'$ satisfies (c)) and hence $0 = 0 + 0' = 0'$ (since 0 satisfies (c)). Hence $0 = 0'$. Therefore the number 0 is completely determined by the requirement that it satisfies (c).

2. Similarly there can only be one number 1 which satisfies rule (g). If you understand the argument which shows that $0 = 0'$ above, then you should have no difficulty in convincing yourself of this.

3. A very reasonable question is why do we impose the strange looking condition $0 \neq 1$? After all, 0 is 0 and 1 is 1, they look totally different. The reason for this is that the number 0 is completely determined by the rule (c) and the number 1 is completely determined by the rule (g); we could conceive of a strange state of affairs in which there was a single number which satisfied *both properties*. We want to exclude this from happening.

4. If $x \in X$ then there is only one number $-x \in \mathbb{R}$ such that $x + (-x) = 0$. Suppose that $x + y = 0$. We will prove that $y = -x$. We have

$$\begin{aligned} & -x + (x + y) = -x + 0 \\ \Longrightarrow\ & (-x + x) + y = -x \quad \text{(by (b) and (c))} \\ \Longrightarrow\ & 0 + y = -x \quad \text{(by (d))} \\ \Longrightarrow\ & y = -x \quad \text{(by (c))}. \end{aligned}$$

5. It follows immediately from observation 4. above that $-(-x) = x$. From (d) we have $x + (-x) = 0$, i.e. $(-x) + x = 0$. Therefore, since $-(-x)$ is the *unique* real number such that $(-x) + (-(-x)) = 0$ by 4., we see that $-(-x) = x$.

6. If $x \in \mathbb{R}$ then $0 \cdot x = 0$. To see this we argue as follows:

$$\begin{aligned} & 0 \cdot x = (0 + 0) \cdot x \quad \text{(by (c))} \\ \Longrightarrow\ & 0 \cdot x = x \cdot (0 + 0) \quad \text{(by (e))} \\ \Longrightarrow\ & 0 \cdot x = x \cdot 0 + x \cdot 0 \quad \text{(by (i))} \\ \Longrightarrow\ & 0 \cdot x = 0 \cdot x + 0 \cdot x \quad \text{(by (e))} \\ \Longrightarrow\ & 0 \cdot x + (-0 \cdot x) = (0 \cdot x + 0 \cdot x) + (-0 \cdot x) \\ \Longrightarrow\ & 0 = 0 \cdot x + (0 \cdot x + (-0 \cdot x)) \quad \text{(by (d) + (b))} \\ \Longrightarrow\ & 0 = 0 \cdot x + 0 \quad \text{(by (d))} \\ \Longrightarrow\ & 0 = 0 \cdot x \quad \text{(by (c))} \end{aligned}$$

7. If $x \in \mathbb{R}$ then $-x = (-1) \cdot x$. To see this observe that

$$\begin{aligned} & 0 = 0 \cdot x \quad \text{(by 6.)} \\ \Longrightarrow\ & 0 = (1 + (-1)) \cdot x \quad \text{(by (d))} \\ \Longrightarrow\ & 0 = 1 \cdot x + (-1) \cdot x \quad \text{(by (i) and (e), twice)} \\ \Longrightarrow\ & 0 = x + (-1) \cdot x. \end{aligned}$$

Therefore, by 5. above it follows that $(-1) \cdot x = -x$.

8. What would happen if we did not impose the requirement that $0 \neq 1$ but we kept all of the rules (a)–(i)? If $x \in \mathbb{R}$ we would have $x = 1 \cdot x$, but if we supposed that $1 = 0$ then we would have $x = 0 \cdot x$, which we have just seen is equal to 0. Hence $x = 0$ for all x. So the only real number would be zero.