If we define addition of natural numbers in a usual way, then it is easy to see that an outcome of adding two natural numbers is a natural number. We then will say that the set $\mathbb{N}$ of natural numbers is closed under addition. On the other hand, if we define the difference of two natural numbers, a and b, as the number $a-b \in \mathbb{N}$ s.t. $b+(a-b)=a$ then this object would only be defined if $a>b$. In order to extend the definition of the difference to $a<b$, we need to enlarge the set of natural numbers to include 0 and negative integers – this gives us the set of all integers $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$. Note that $\mathbb{N} \subset \mathbb{Z}$ and $\mathbb{Z}$ is closed under subtraction.

In $\mathbb{Z}$ we can define multiplication in the usual way where it is clear that $a,b \in \mathbb{Z} \Rightarrow ab \in \mathbb{Z} \Rightarrow$ $\mathbb{Z}$ is closed under multiplication. However, $\mathbb{Z}$ is not closed under division: $1/2 \notin \mathbb{Z}$. We enlarge $\mathbb{Z}$ by introducing the set of rational numbers $\mathbb{Q}$ as follows

$$\mathbb{Q} = \left\{ \frac{m}{n} : m,n \in \mathbb{Z}; n \neq 0 \right\}$$

Here we assume that:

(1) $\frac{m}{n} = \frac{km}{kn}$ if $k \neq 0, k \in \mathbb{Z}$, (2) $\frac{0}{n} = 0$, (3) $\frac{m}{1} = m$,

(4) $\frac{m}{n}\frac{k}{\ell} = \frac{mk}{n\ell}$, (5) $\frac{m}{n} + \frac{k}{\ell} = \frac{m\ell + nk}{n\ell}$, (6) $\left(\frac{m}{n}\right)^{-1} = \frac{n}{m}$ if $m,n \neq 0$

From (1) it follows that the same rational number can be written in infinitely many ways; If m and n do not have common factors, we say that the fraction is irreducible. From (3) it follows that $\mathbb{Z} \subset \mathbb{Q}$ and the remaining properties ensure that $\mathbb{Q}$ is closed under operations: "+", "−", "*", and "÷". It would appear then that $\mathbb{Q}$ would be a sufficiently large set of numbers for practical applications. However, as it is well-known this is not so.

One immediate deficiency that one encounters is associated with solving equations: as we will demonstrate shortly, numbers such as $\sqrt{2}$, $\sqrt{17}$ cannot be rational so that the equations $x^2 = 2$, $x^2 = 17$ that appear is applications do not have rational solutions. Other deficiencies exist but we will discuss them in the next lecture.

We will now discuss a systematic approach to demonstrating that solution of certain polynomial equations cannot be rational.

Definition: A number r is called algebraic if it satisfies a polynomial equation with integer coefficients, i.e., if there exist a natural number n and integers $a_0, \dots, a_n \in \mathbb{Z}$

s.t. $a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = 0$.

Then $\sqrt{z}$ is an algebraic number since it solves the equation $x^2 - z = 0$. Similarly, if $z = \sqrt{1+\sqrt[3]{15}}$, then

$z^2 = 1+\sqrt[3]{15} \Rightarrow z^2 - 1 = \sqrt[3]{15} \Rightarrow (z^2-1)^3 = 15 \Rightarrow z^6 - 3z^4 + 3z^2 - 1 = 15$

$\Rightarrow z^6 - 3z^4 + 3z^2 - 16 = 0$ – z is a solution of a polynomial equation with integer coefficients and thus is an algebraic number.

We have the following:

<u>Rational Zeroes Theorem.</u> Suppose $z = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $q \neq 0$ is an irreducible fraction that satisfies the equation

$$(*) \qquad a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0,$$ where

$a_0, \dots, a_n \in \mathbb{Z}$ with $a_0, a_n \neq 0$. Then p divides a_0 and q divides a_n.

<u>Proof:</u> Substituting z into $(*)$, we have

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \frac{p}{q} + a_0 = 0$$

Multiplying this equation by q^n, we get

$$(**) \qquad a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$$

We can factor out p from the first n terms in $(**)$ to get

$$p\left(a_n p^{n-1} + a_{n-1} p^{n-2} q + \dots + a_1 q^{n-1}\right) = -a_0 q^n$$

$\Rightarrow$ $a_0 q^n$ must be divisible by p $\Rightarrow$ either a_0 is divisible by p or q^n is divisible by p. However, p and q have no common factors $\Rightarrow$ a_0 is divisible by p. Now, factor q from the last n terms in (**):

$$a_n p^n = -q\left(a_{n-1}p^{n-1} + a_{n-2}\,q\,p^{n-2} + \dots + a_1 q^{n-2} p + a_0 q^{n-1}\right)$$

We use the same logic: $a_n p^n$ is divisible by q, but p and q have no common factors hence p^n cannot be divided by q $\Rightarrow$ a_n is divisible by q $\blacksquare$

Examle: $\sqrt{2}$ is not rational $\Rightarrow$ let $x = \sqrt{2}$ $\Rightarrow$ $x^2 = 2$ $\Rightarrow$ $\boxed{x^2 - 2 = 0}$. Assume that x is rational, i.e., there exist integers p and q s.t. $x = \frac{p}{q}$. Then, by RZT: q divides 1 and p divides -2 $\Rightarrow$ $q = \pm 1$ and $p = \pm 1, \pm 2$ $\Rightarrow$ Possible choices of $\frac{p}{q}$: $\pm 1, \pm 2$ $\Rightarrow$ $x = \pm 1$ or ± 2. However $(\pm 1)^2 - 2 = -1$ and $(\pm 2)^2 - 2 = 2$ $\Rightarrow$ Neither choice of x satisfies $x^2 - 2 = 0$ $\Rightarrow$ no rational solutions $\Rightarrow$ $\sqrt{2}$ is not rational.

Example: Show that $r = \sqrt{1 + \sqrt[3]{15}}$ is not rational.

We already showed: $z^6-3z^4+3z^2-16=0$. Assume $z=\frac{p}{q}$, where p,q are integers and the fraction is irreducible.

RZT: p divides 16 and q divides 1 $\Rightarrow$ $q=\pm 1$ and

$p=\pm1, \pm2, \pm4, \pm8, \pm16 \Rightarrow z=\frac{p}{q}=\pm1, \pm2, \pm4, \pm8, \pm16$

If $z=\pm1$: $1-3+3-16=-15\neq 0$

If $z=\pm2$: $64-3\cdot16+3\cdot4-16=12\neq0$

$\vdots$

– no rational solutions for the polynomial equation $\Rightarrow$

z is not rational.