0. Throughout this handout we are going to study rational numbers and irrational numbers. They are viewed as various types of real numbers.

   We (tacitly) assume what we have learnt in school maths about addition, subtraction, multiplication and division for real numbers.

   We further (tacitly) assume what we have learnt in school maths about surds of (positive) real numbers.

   We also (tacitly) assume what we have learnt in school maths about addition, subtraction, multiplication for integers.

1. **Definition. (Rationals.)**

   Let $x \in \mathbb{R}$. We say that x is a **rational number** *if there exist some $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $m = nx$.*

   Remark on notation and terminology.

   (a) When it happens that x is a rational number and m, n are integers which satisfy $n \neq 0$ and $m = nx$, we are allowed to write $x = \dfrac{m}{n}$. In this situation, we agree to say the rational number x is represented as the fraction (of integers) 'the integer m over the integer n'.

   Note that the same rational number admits many different representations as fractions of integers. (For example, 0.5 can be represented as $\cdots, \dfrac{-3}{-6}, \dfrac{-2}{-4}, \dfrac{-1}{-2}, \dfrac{1}{2}, \dfrac{2}{4}, \dfrac{3}{6}, \cdots$.)

   (b) We collect all rational numbers together to form the 'set of all rational numbers'. This set is denoted by $\mathbb{Q}$. By construction $\mathbb{Q}$ is a subset of $\mathbb{R}$.

2. **Theorem (1). (Addition, subtraction, multiplication and division for rational numbers.)**

   Let x, y are real numbers. The statements below hold:

   (a) *Suppose x, y are rational numbers. Then $x + y$ is a rational number.*

   (b) *Suppose x, y are rational numbers. Then $x - y$ is a rational number.*

   (c) *Suppose x, y are rational numbers. Then xy is a rational number.*

   (d) *Suppose x, y are rational numbers, and $y \neq 0$. Then $\dfrac{x}{y}$ is a rational number.*

   Proof of Theorem (1). Exercise. (Imitate what has been done in the handout *Basic results on divisibility*.)

3. **'Laws of arithmetic' for rational numbers.**

   Very often we tend to view Theorem (1) as a part of Theorem (2), which are collectively referred to as the 'usual laws of arithmetic' for rational numbers. The rest of Theorem (2) is simply a consequence of a 'restriction' of the laws of arithmetic for real numbers to the special case of rational numbers.

   Theorem (2).

   (a) *For any $x, y \in \mathbb{Q}$, $x + y \in \mathbb{Q}$.*

   (b) *For any $x, y, z \in \mathbb{Q}$, $(x + y) + z = x + (y + z)$.*

   (c) *There exists some $\kappa \in \mathbb{Q}$, namely $\kappa = 0$, such that for any $x \in \mathbb{Q}$, $\kappa + x = x$ and $x + \kappa = x$.*

   (d) *For any $x \in \mathbb{Q}$, there exists some $y \in \mathbb{Q}$, namely $y = -x$, such that $x + y = 0 = y + x$.*

   (e) *For any $x, y \in \mathbb{Q}$, $x + y = y + x$.*

   (f) *For any $x, y \in \mathbb{Q}$, $xy \in \mathbb{Q}$.*

   (g) *For any $x, y, z \in \mathbb{Q}$, $(xy)z = x(yz)$.*

   (h) *There exists some $\lambda \in \mathbb{Q}$, namely $\lambda = 1$, such that for any $x \in \mathbb{Q}$, $\lambda x = x$ and $x\lambda = x$.*

   (i) *For any $x \in \mathbb{Q}$, if $x \neq 0$, then there exists some $y \in \mathbb{Q}$, namely $y = \dfrac{1}{x}$, such that $xy = 1$ and $yx = 1$.*

   (j) *For any $x, y \in \mathbb{Q}$, $xy = yx$.*

   (k) *For any $x, y, z \in \mathbb{Q}$, $x(y + z) = xy + xz$.*

(l) *For any* $x, y, z \in \mathbb{Q}$, $(y+z)x = yx + zx$.

4. **Definitions. (Irrationals.)**

   Let $x \in \mathbb{R}$. *We say that* x *is an* **irrational number** *if* x *is not a rational number.*

   Comment. The 'defining condition' in the definition for the notion of irrationals, namely '*x is not a rational number*', makes it difficult to use in arguments. Arguments for statements involving irrational numbers necessitates the use of the method of proof-by-contradiction.

   We shall give a few simple examples of this type of arguments, each concerned with a statement involving irrational numbers.

5. **Statement (a).**

   Let a, b, c, u *be positive real numbers. Suppose* a, b, c *are rational and* $au^2 + bu + c$ *is irrational. Then* u *is an irrational number.*

   Proof of Statement (a), constructed with the method of proof-by-contradiction.

   Let a, b, c, u be positive real numbers. Suppose a, b, c are rational and $au^2 + bu + c$ is irrational. [We have stated the assumption to be used throughout the argument.]

   Further suppose it were true that u was a rational number.

   > [*Reminder.* We have just announced, for the sake of argument, we for the moment assumed that the desired conclusion
   >
   > '*u is an irrational number*'
   >
   > fails to hold.
   > We are going to look for something 'ridiculously wrong', called a contradiction, out of the combination of what we have supposed and what we have further supposed.
   > Then we will be made to conclude that under the assumption
   >
   > '*a, b, c, u are positive real numbers, a, b, c, are rational, and $au^2 + bu + c$ is irrational*',
   >
   > the desired conclusion
   >
   > '*u is an irrational number*'
   >
   > is 'forced' to follow.]

   Since u was rational, u^2 would also be rational.

   Now, since b, u were rational, bu would be rational.

   Moreover, Since a, u^2 were rational, au^2 would be rational.

   Then, since au^2, bu, c were rational, $au^2 + bu + c$ would be rational.

   Recall that $au^2 + bu + c$ is an irrational number by assumption.

   Then $au^2 + bu + c$ would be simultaneously a rational number and not a rational number. [This is something 'ridiculously wrong'.]

   Contradiction arises.

   It follows that, in the first place, u is an irrational number.

6. **Statement (b).**

   Let a, u *be positive real numbers. Suppose* a *is rational and* u *is irrational. Then* $\sqrt{a+u}$ *is an irrational number.*

   Proof of Statement (b), constructed with the method of proof-by-contradiction.

   Let a, u be positive real numbers. Suppose a is rational and u is irrational. [We have stated the assumption to be used throughout the argument.]

   Further suppose it were true that $\sqrt{a+u}$ was a rational number.

   > [*Reminder.* We have just announced, for the sake of argument, we for the moment assumed that the desired conclusion
   >
   > '*$\sqrt{a+u}$ is an irrational number*'

fails to hold.

We are going to look for something 'ridiculously wrong', called a contradiction, out of the combination of what we have supposed and what we have further supposed.

Then we will be made to conclude that under the assumption

'*a, u are positive real numbers, a is rational, and u is irrational*',

the desired conclusion

'*$\sqrt{a+u}$ is an irrational number*'

is 'forced' to follow.]

Since a, u are positive real numbers, $a+u$ is also a positive real number. Then $(\sqrt{a+u})^2 = a+u$.

By assumption, $\sqrt{a+u}$ was rational. Then $a+u$ would be rational.

Now, since $a, a+u$ were rational and $u = (a+u) - a$ were rational, u would be rational.

Recall that u is an irrational number by assumption.

Then u would be simultaneously a rational number and not a rational number. [This is something 'ridiculously wrong'.]

Contradiction arises.

It follows that, in the first place, $\sqrt{a+u}$ is irrational.

7. **Statement (c).**

   Suppose a, b are rational numbers and $b \neq 0$. Then $a + b\sqrt{2}$ is an irrational number.

   Remark. Here we take for granted that $\sqrt{2}$ is an irrational number.

   Proof of Statement (c), constructed with the method of proof-by-contradiction.

   Suppose a, b are rational numbers and $b \neq 0$. [We have stated the assumption to be used throughout the argument.]

   Further suppose it were true that $a + b\sqrt{2}$ was a rational number.

   [We are going to look for a contradiction out of the combination of what we have supposed and what we have further supposed.]

   Write $r = a + b\sqrt{2}$.

   By assumption, a, r were rational numbers and $b\sqrt{2} = r - a$. Then $b\sqrt{2}$ would be a rational number.

   By assumption, b is a non-zero rational number. Also note that $\sqrt{2} = \dfrac{b\sqrt{2}}{b}$. Then $\sqrt{2}$ would be a rational number.

   Recall that $\sqrt{2}$ is an irrational number.

   Then $\sqrt{2}$ would be simultaneously a rational number and not a rational number.

   Contradiction arises.

   It follows that, in the first place, $a + b\sqrt{2}$ is an irrational number.

8. **Statement (d).**

   Let a, b, c, d be rational numbers. Suppose $a + b\sqrt{3} = c + d\sqrt{3}$. Then $a = c$ and $b = d$.

   Remark. Here we take for granted that $\sqrt{3}$ is an irrational number.

   Proof of Statement (d), with an application of the method of proof-by-contradiction embedded.

   Let a, b, c, d be rational numbers. Suppose $a + b\sqrt{3} = c + d\sqrt{3}$.

   [*Roughwork.* It would be perfectly fine to *choose* to write

   '*further suppose it were true that $a \neq c$ or $b \neq d$*',

   and proceed to obtain a contradiction out of the combination of the assumption above and this further assumption.

   But this is not clever, because the presence of the word '*or*' would mean we had to consider various cases.

   So we do something else first.]

By assumption, $a - c = (d - b)\sqrt{3}$.

We verify that $b = d$, with the method of proof-by-contradiction:

- Suppose it were true that $b \neq d$.

  [We are going to look for a contradiction out of the combination of what we have supposed and what we have just further supposed.]

  Then $d - b \neq 0$ also. Then $\dfrac{a-c}{d-b}$ would be well-defined as a real number.

  Since a, b, c, d are rational numbers, each of $a - c$, $b - d$, $\dfrac{a-c}{d-b}$ is a rational number.

  Since $a - c = (d - b)\sqrt{3}$, we would have $\dfrac{a-c}{d-b} = \sqrt{3}$.

  Then $\sqrt{3}$ would be a rational number.

  Recall that $\sqrt{3}$ is an irrational number. Then $\sqrt{3}$ is simultaneously a rational number and not a rational number.

  Contradiction arises.

  It follows that, in the first place, $b = d$.

Now, as $b = d$, we have $d - b = 0$. Then $a - c = (d - b)\sqrt{3} = 0$. Hence $a = c$ also.

9. **Surds of positive prime numbers.**

   Recall the definition for the notion of *prime numbers*:

   Let p be an integer. Suppose $p \neq -1$ and $p \neq 0$ and $p \neq 1$. Then we say p is a prime number if the statement (PR) holds:

   (PR) *p is divisible by no integer other than $1, -1, p, -p$.*

   Theorem (3). (Irrationality of surds of positive prime numbers.)

   Suppose n is an integer greater than 1, and p is a positive prime number. Then $\sqrt[n]{p}$ is an irrational number.

   Remark. As a consequence of Theorem (3), the numbers $\sqrt{2}$ and $\sqrt{3}$ are indeed irrational numbers.

10. **Euclid's Lemma and the irrationality of surds of positive prime numbers.**

    The proof of Theorem (3) relies on the validity of a result, known as Euclid's Lemma, which we have likely taken for granted since childhood.

    Euclid's Lemma.

    Let $h, k \in \mathbb{Z}$, and p be a prime number. Suppose hk is divisible by p.

    Then at least one of h, k is divisible by p.

    Remarks.

    (a) Euclid's Lemma is a non-trivial result. Its proof will be postponed.

    (b) The proof of Theorem (3) (as an application of Euclid's Lemma) will be left as an exercise. Just imitate the self-contained proof of Statement (e).

11. For covenience we also introduce the notion of *common divisor*. It will be used in the proof of Theorem (3).

    Definition. (Common divisor.)

    Let m, n, c be integers. We say that c is a common divisor of m, n if m is divisible by c and n is divisible by c.

12. **Statement (e).**

    $\sqrt{2}$ is an irrational number.

    Proof of Statement (e).

    Suppose it were true that $\sqrt{2}$ was a rational number.

    Then there would exist some $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $n\sqrt{2} = m$.

    Without loss of generality, we assume that m, n have no common divisor other than $1, -1$; (otherwise, cancel all common divisors of m, n as numerators, denominators in the fraction $\dfrac{m}{n}$ to obtain $\dfrac{m'}{n'}$ and then re-label m', n' as m, n respectively).

Since $\sqrt{2} = \dfrac{m}{n}$, we would have $m^2 = 2n^2$.

Since $n^2 \in \mathbb{Z}$, m^2 would be divisible by 2.

According to Euclid's Lemma, m would be divisible by 2.

Then there would exist some $k \in \mathbb{Z}$ such that $m = 2k$.

Therefore, for the same m, n, k, we would have $2n^2 = (2k)^2 = 4k^2$.

Hence $n^2 = 2k^2$.

Repeating the above argument, we deduce that n would be divisible by 2.

Now 2 would be a common divisor of m and n.

But recall that m, n have no common divisor other than $1, -1$.

Contradiction arises.

It follows that, in the first place, $\sqrt{2}$ is an irrational number.

13. **Alternative proof of Statement (e).**

Suppose it were true that $\sqrt{2}$ was a rational number.

Then there would exist some $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $n \cdot \sqrt{2} = m$.

By assumption we would have $m^2 = 2n^2$.

- Since $n^2 \in \mathbb{Z}$, m^2 would be divisible by 2.
  According to Euclid's Lemma, m would be divisible by 2.
  Then there would exist some $k_0 \in \mathbb{Z}$ such that $m = 2k_0$.
  Therefore, for the same m, n, k_0, we would have $2n^2 = m^2 = (2k_0)^2 = 4{k_0}^2$.
  Hence $n^2 = 2{k_0}^2$. Note that $k_0 \neq 0$ (because $n \neq 0$).
- Repeating the above argument, we deduce that n would be divisible by 2.
  Then there would exist some $k_1 \in \mathbb{Z}$ such that $n = 2k_1$.
  Therefore, for the same n, k_0, k_1, we would have $2{k_0}^2 = n^2 = (2k_1)^2 = 4{k_1}^2$.
  Hence ${k_0}^2 = 2{k_1}^2$. Note that $k_1 \neq 0$ (because $k_0 \neq 0$).
- Repeating the above argument, we deduce that k_0 would be divisible by 2.
  Then there would exist some $k_2 \in \mathbb{Z}$ such that $k_0 = 2k_2$.
  Further repeating the above argument, we deduce that ${k_1}^2 = 2{k_2}^2$. Note that $k_2 \neq 0$.

Hence repeating the argument *ad infinitum*, we obtain an infinite sequence of non-zero integers $\{k_j\}_{j=0}^{\infty}$ which satisfies ${k_j}^2 = 2{k_{j+1}}^2$ for each j.

Then $\{{k_j}^2\}_{j=0}^{\infty}$ is an infinite sequence of positive integers which is strictly decreasing.

But such an infinite sequence cannot exist. (Why?) Contradiction arises.

It follows that, in the first place, $\sqrt{2}$ is an irrational number.

Remark. What brings about the desired contradiction is something known as the **Well-ordering Principle for Integers**, which is one of the 'fundamental beliefs' in mathematics:

> *Let S be a subset of $\mathbb{N}$. Suppose S is non-empty. Then S has a least element.*

We will formally introduce it later in the course.

14. **Digression on logic: Proof-by-contradiction argument.**

Re-examine the proof-by-contradiction argument for Statement (a), Statement (b), and Statement (c) in this handout.

Each of these statements is of the form:

> **Let** *blah-blah-blah.* **Suppose** *bleh-bleh-bleh.* **Then** *blih-blih-blih.*

The general format for a proof-by-contradiction argument for such a statement is:

Let *blah-blah-blah.* **Suppose** *bleh-bleh-bleh.*

Further suppose that it is not true that *'blih-blih-blih' holds.*

Then so-and-so, so-and-so, so-and-so. (This is the main body of the argument, leading towards a desired contradiction.)

Contradiction arises.

It follows that, in the first place, *'blih-blih-blih' holds.*

What is written at each 'intermediate step' in the 'main body of the argument' will have, as its justification, something assumed at the top, or already established within this passage, or something known to be 'true in general'.

We postpone the discussion on the mechanism behind this method of argument until we know more about mathematical logic.