Weeks 8 and 9: Irrational Numbers

Jiahan

1 Basic Definitions

Today we investigate irrational numbers. Recall that we have the set of integers:

$$..., -3, -2, -1, 0, 1, 2, 3, ...$$

Two positive integers are said to be **coprime** if their greatest common divisor is 1. A real number r is called **rational** if $r = \frac{p}{q}$ for some integers p, q with q nonzero; r is called **irrational** if otherwise. Notice that if a positive rational number $r = \frac{p}{q}$ for positive integers p, q, then we may assume that p, q are coprime by dividing out the greatest common divisor of p and q.

Exercise 0: Is 2022 rational? What about -0.4? What about $\frac{5}{2}$?

Example 1: $\sqrt{2}$ is irrational.

Proof: if $\sqrt{2} = \frac{p}{q}$, where p, q are coprime positive integers, then $p^2 = 2q^2$, hence p is even. Let $p = 2m$, then $2m^2 = q^2$, then q is even. This contradicts the fact that p, q are coprime.

Exercise 2: Which of the following numbers are irrational?
(a) $\sqrt[3]{2}$,
(b) $\sqrt{2} + \sqrt{3}$
(c) $\log_{10} 2$.
(d) $\sqrt{2 + 2\sqrt{2}}$.

Exercise 3: Prove that if a real number can be expressed as $p + q\sqrt{2}$ where p, q are rational, then it has a unique such expression.

We state the following theorem without proof. However, if there is time, you can try to prove it by assuming $x = \frac{m}{n}$ for $m, n \in \mathbb{Z}$, then multiply by n^k.

Theorem 4: In general, if $p(x)$ is a polynomial of the form $p(x) = a_k x^k + a_{k-1} x^{k-1} + ... + a_1 x^1 + a_0$, where a_i, $i = 0, ..., k$ are integers, $a_n \neq 0$, then if $\frac{m}{n}$ is a root of $p(x) = 0$, where m, n are integers such that $|m|$ and $|n|$ are coprime and $n \neq 0$, then m divides a_0 and n divides a_k.

Exercise 5: Prove that the $x^7 - 4x - 1 = 0$ has no real rational roots.

However, in general determining if something is rational or not is extremely difficult; famously it is still open whether $\pi + e, \pi - e, \pi \cdot e, \ln \pi$ are irrational or not.

2 Approximating Irrationals by Fractions

Irrationals can be approximated by rationals. For example, $\sqrt{2} = 1.414213...$, so we can have the following approximation

$$1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}...$$

However, these are bad approximations. For example, you can check that $\left|\frac{17}{12} - \sqrt{2}\right| < 0.00246$, however $\left|\frac{141}{100} - \sqrt{2}\right| = 0.0042...$, so $\frac{17}{12}$ is a much better approximation to $\sqrt{2}$ than $\frac{141}{100}$, even though the first one has much smaller denominator (12) than that of the second one (100). Another problem is that a priori we don't know the decimal expansions of $\sqrt{2}$, hence we cannot get approximations like $1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}...$ without first use a calculator to see what $\sqrt{2}$ is. A third problem is that we would like to have some sort of error estimation on our approximation.

The way to proceed is as follows:

$0 < \sqrt{2} - 1 < \frac{1}{2}$, this is obvious.

Square both sides: $0 < 3 - 2\sqrt{2} < \frac{1}{4}$,

this rearranges to $0 < \frac{3}{2} - \sqrt{2} < \frac{1}{8}$! Something miraculous has happened, start with an approximation with error bound $\frac{1}{2}$, we got an approximation with error bound $\frac{1}{8}$!

Square $0 < 3 - 2\sqrt{2} < \frac{1}{4}$ one more time, we get $0 < 17 - 12\sqrt{2} < \frac{1}{16}$, this rearranges to $0 < \frac{17}{12} - \sqrt{2} < \frac{1}{192}$! What a ridiculously efficient way of computing $\sqrt{2}$.

Exercise 6: Find a fraction that approximates $\sqrt{2}$ to within 10^{-20}. Do the same with $\sqrt{5}$. Surprisingly, you don't need many iterations to achieve such high accuracy.

Just how good is our result precisely? The following argument shows that this is the best possible.

Example 7: Recall $\frac{17}{12}$ approximates $\sqrt{2}$ to within 0.00246, if $\frac{p}{q}$ with p, q coprime is another fraction that approximates $\sqrt{2}$ to within 0.00246, then from the triangle inequality, we have:

$$\left|\frac{p}{q} - \frac{17}{12}\right| \leq \left|\frac{p}{q} - \sqrt{2}\right| + \left|\frac{17}{12} - \sqrt{2}\right| \leq 0.00246 + 0.00246 = 0.00492.$$

However, $\left|\frac{p}{q} - \frac{17}{12}\right| = \left|\frac{12p-17q}{12q}\right| \geq \frac{1}{12q}$, hence $\frac{1}{12q} \leq 0.00492$, so $q \geq 16.9...$, so $q \geq 17$! i.e., if you want a fractional that approximates $\sqrt{2}$ better than $\frac{17}{12}$, you need one with denominator at least 17!

Exercise 8: Repeat the process above for π and $\frac{355}{113}$. You may use the fact that $\frac{355}{113}$ approximates π to within 2.67×10^{-7}. You may be in for a surprise.

The process above is related to continued fractions. Our approximations to $\sqrt{2}$ obtained by keep squaring stuff can also be obtained by using continued fractions. It is possible to show that continued fractions give the best approximations possible. Similarly, $\frac{355}{113}$ can be obtained by using continued fraction as well. The topic of approximating reals by rationals is called **Diophantine approximation**.

Exercise 9: Modify our method to obtain rational approximation to $\sqrt[3]{2}$.[1]

3 Algebraic Numbers and Transcendental Numbers

Definition 10: A real number is called an **algebraic number** if it is the root of a nonzero polynomial with integer coefficients. It is called a **transcendental number** if otherwise.

Of course transcendental numbers are irrational.

Exercise 11: Prove the following numbers are all algebraic numbers: $\sqrt{2}+\sqrt{3}$, $\sqrt{2}+\sqrt{3}+\sqrt{5}$, $\sqrt{2}+\sqrt[3]{3}$.

Does your method above work for showing $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ is an algebraic number?

The **Gelfond-Schneider theorem** says if a is an algebraic number that is not 0 or 1, b is irrational algebraic, then a^b is transcendental. We won't be proving this statement, however for an application:

Exercise 12: Prove that $\log_{10} 2$ is a transcendental number.

Theorem 13: If α, β are both algebraic numbers, then $\alpha+\beta, \alpha\cdot\beta$ are both algebraic numbers.

You can use the theorem to convince yourself that $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ is indeed an algebraic number despite not being immediately obvious.

Optional and time permitting: We will devote all of our remaining time and effort to the proof of this theorem. Our proof is constructive and will give a stronger statement.

Proof of theorem 13:

1) First, to illustrate the point, let us first suppose α is the root of $\alpha^2-\alpha-1=0$, then we can express α^2 as $\alpha+1$. We can also write $\alpha^3=\alpha\cdot\alpha^2=\alpha(\alpha+1)=\alpha^2+\alpha=\alpha+1+\alpha=2\alpha+1$. Inductively, we can express α^n as a linear combination of α and 1 for any positive integer n.

2) Mimic step 1), prove that if α is the root of a polynomial $a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0=0$ with integer coefficients, then α^k can be written as an integral linear combination of $\alpha^{n-1},...,\alpha,1$ for all nonnegative integers k.

3) Prove if α,β are roots to $a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0=0$ and $b_my^m+b_{m-1}y^{m-1}+...+b_1y+b_0=0$, then $\alpha^k\beta^p$ can be written as an integer linear combination of $\alpha^i\beta^j, 0\le i\le n-1, 0\le j\le m-1$ for any nonnegative integers k,p.

4) With the assumptions and notations as in step 3), prove that $(\alpha+\beta)^q$ can be written as an integer linear combination of $\alpha^i\beta^j, 0\le i\le n-1, 0\le j\le m-1$ for any

[1] The same iterative procedure can also be obtained from Newton's method.

nonnegative integer q.

5) Now we need a technical lemma: If $d_{i,j}, 1 \le i \le n, 1 \le j \le m$ with $\boldsymbol{n < m}$ is a collection of integers, then we can find integers $e_j, 1 \le j \le m$ such that e_j's are **not all zero** and $\sum_j d_{i,j} e_j = 0$ for all i.

6) To see why the lemma above is correct, consider a simple example $n = 1, m = 2$, $d_{1,1} = 2, d_{1,2} = 3$, then clearly $2e_1 + 3e_2 = 0$ has a integer solution e_1, e_2 such that they are not all zero. For a more sophisticated example like

$$\begin{cases} 2e_1 + e_2 - e_3 = 0 \\ 3e_1 - 2e_2 + e_3 = 0, \end{cases} \tag{1}$$

we can simply eliminate one variable, say e_1, by multiplying the top equation by 3 then subtract from it the bottom equation times 2. Then we have reduced this system of linear equations into just one simple equation, which has a nonzero integer solution, from which we can recover a nonzero rational solution e_1, e_2, e_3; then it must have a nonzero integer solution for e_1, e_2, e_3 by multiplying them with an integer.

7) Depending on if I have convinced you of the correctness of 5) by the two examples in 6), you can either rigorously prove 5) by following the same inductive method in 6) or move on.

8) We have now set the stage for proving that sums and products of algebraic numbers are algebraic using 3),4) and 5).

Instead of burying you in notations and indices, again I shall illustrate the method by an example, and you should fill in the details. Suppose $\alpha^2 - \alpha - 1 = 0$ and $\beta^2 - 2 = 0$; we would like to show that $\alpha + \beta$ is the root of a polynomial of degree at most 4 with integer coefficients. To wit, we would like to find five integers c_4, c_3, c_2, c_1, c_0 such that

$$c_4(\alpha+\beta)^4 + c_3(\alpha+\beta)^3 + c_2(\alpha+\beta)^2 + c_1(\alpha+\beta) + c_0 = 0. \qquad *$$

By step 4), each $(\alpha+\beta)^i, i = 0, ..., 4$ is an integer linear combination of $\alpha\beta, \alpha, \beta$ and 1. Therefore, equation $*$ can be regrouped as

$$(...)\alpha\beta + (...)\alpha + (...)\beta + (...) = 0$$

where each (...) is a linear combination of $c_4, c_3, ., .., c_0$ with **known integer coefficients**. By setting each (...) to zero individually, we now invoke step 5) to argue that we can find integers $c_4, ..., c_0$ not all zero that satisfies equation $*$.

9) Depending on if I have convinced you of theorem 13 with example 8), you can either stop here or prove the theorem more completely using the method sketched above in 8). Note that we have proven the stronger statement: if α is the root of an integer coefficient polynomial of degree m, β is the root of an integer coefficient polynomial of degree n, then $\alpha + \beta, \alpha \cdot \beta$ are roots of integer coefficients polynomials of degrees at most mn.