Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 27, 2023

What we have seen last lecture

- Divisor set
- Multiplicative functions
- Euclid-Euler theorem

Today's topics

- Rational numbers
- Irrational numbers
- Algebraic numbers

Part III

Rational and Algebraic Numbers

Rational numbers

Rational numbers

Definition 8.1

A ***fraction*** is an expression of the form $\frac{a}{b}$, where a, b are integers and $b \neq 0$. A ***rational number*** is a number which can be expressed by a fraction.

Example 8.2

$\frac{5}{3}$ and $\frac{15}{9}$ are two distinct fractions, but they express the same rational number. “$\frac{5}{3} = \frac{15}{9}$”.

Rational numbers

Definition 8.1

A ***fraction*** is an expression of the form $\frac{a}{b}$, where a, b are integers and $b \neq 0$. A ***rational number*** is a number which can be expressed by a fraction.

Example 8.2

$\frac{5}{3}$ and $\frac{15}{9}$ are two distinct fractions, but they express the same rational number. "$\frac{5}{3} = \frac{15}{9}$".

Definition 8.3

A ***fraction*** $\frac{a}{b}$ is ***reduced*** if a, b are coprime and $b > 0$.

Example 8.4

$\frac{-5}{3}$ is reduced, $\frac{5}{-3}$ is not reduced, and $\frac{-15}{9}$ is not reduced.

Rational numbers

Theorem 8.5

Any rational number can be uniquely expressed by a reduced fraction.

$$\frac{15}{-9} = \frac{-5}{3} \leftarrow \text{reduced !}$$

Theorem 8.5

Any rational number can be uniquely expressed by a reduced fraction.

Proof. Let's assume our rational number is expressed by $\frac{a}{b}$. Since $\frac{a}{b} = \frac{-a}{-b}$, we may assume $b > 0$. Let $c = \frac{a}{\gcd(a,b)}$ and $d = \frac{b}{\gcd(a,b)}$. Then $\gcd(c, d) = 1$ and we have $\frac{a}{b} = \frac{c}{d}$. ← reduced.

Theorem 8.5

Any rational number can be uniquely expressed by a reduced fraction.

Proof. Let's assume our rational number is expressed by $\frac{a}{b}$. Since $\frac{a}{b} = \frac{-a}{-b}$, we may assume $b > 0$. Let $c = \frac{a}{\gcd(a,b)}$ and $d = \frac{b}{\gcd(a,b)}$. Then $\gcd(c, d) = 1$ and we have $\frac{a}{b} = \frac{c}{d}$.

Now, suppose $\frac{c'}{d'}$ is another reduced fraction such that $\frac{a}{b} = \frac{c'}{d'}$. Then we have $c'd = cd'$. Hence, $d \mid cd'$ and $d' \mid c'd$. Since $\gcd(c, d) = 1$ and $\gcd(c', d') = 1$, we have $d \mid d'$ and $d' \mid d$. Since both d, d' are positive, by the antisymmetry of $\mid$, $d = d'$. Then $c = c'$ and thus $\frac{c}{d}$ and $\frac{c'}{d'}$ are the same fraction. $\square$

Rational numbers

We can extend prime factorization from to rational numbers.

Theorem 8.6 (Prime factorization)

Let α be a positive rational number.

1. *(existence) α admits a prime factorization, i.e. there exist integers e_p for each prime p such that*

   could be negative

$$\alpha = \prod_{p \text{ is prime}} p^{e_p}$$

2. *(uniqueness) Suppose α admits another prime factorization, say*

$$\alpha = \prod_{p \text{ is prime}} p^{f_p}.$$

   Then, for every prime p, we have $e_p = f_p$.

Proof. (***existence***) Let $\frac{a}{b}$ be any fraction expressing α. We may assume a, b are positive. Then by the fundamental theorem of arithmetic,

$$a = \prod_{p \text{ is prime}} p^{v_p(a)}, \qquad b = \prod_{p \text{ is prime}} p^{v_p(b)}.$$

Hence, $\alpha = \dfrac{a}{b} = \dfrac{\prod_{p \text{ is prime}} p^{v_p(a)}}{\prod_{p \text{ is prime}} p^{v_p(b)}} = \displaystyle\prod_{p \text{ is prime}} p^{v_p(a)-v_p(b)}$.

Note that the integer $v_p(a) - v_p(b)$ does not depend on the choice of the fraction $\frac{a}{b}$. Indeed, if $\frac{a'}{b'}$ is another fraction expressing α, then we have $ab' = a'b$. Hence, for all prime p,

$$v_p(a) + v_p(b') = v_p(a') + v_p(b).$$

Therefore, $v_p(a') - v_p(b') = v_p(a) - v_p(b)$. We will denote this integer by $v_p(\alpha)$.

(***uniqueness***) Suppose $\alpha = \prod_{p \text{ is prime}} p^{f_p}$. Let

$$c = \prod_{p \text{ is prime}, f_p > 0} p^{f_p}, \qquad d = \prod_{p \text{ is prime}, f_p < 0} p^{-f_p}.$$

Then $\frac{c}{d}$ is a reduced fraction expressing α. Note that we always have $v_p(c) - v_p(d) = f_p$. Hence, $f_p = v_p(\alpha)$. □

$f_p > 0 \Rightarrow v_p(c) = f_p \;\&\; v_p(d) = 0$

$f_p < 0 \Rightarrow v_p(c) = 0 \;\&\; v_p(d) = f_p$

$f_p = 0 \Rightarrow v_p(c) = v_p(d) = 0$

Example

Example 8.7

Find the reduced fraction expression of the following rational number and give its prime factorization:

$$-1.56$$

$$-1.56 = \frac{-156}{100} = \frac{-39}{25} = -3^1 \cdot 5^{-2} \cdot 13^1$$

Irrational numbers

Irrational numbers

Definition 8.8

If a number is not rational, then it is ***irrational***.

Irrational numbers

Definition 8.8

If a number is not rational, then it is ***irrational***.

Example 8.9

(Pythagorean or Hippasus, 500 BC) $\sqrt{2}$ is irrational.

Proof. Suppose $\sqrt{2}$ is rational and can be expressed by the reduced fraction $\frac{a}{b}$. Then we have

$$2 = \frac{a^2}{b^2}.$$

But since a, b are coprime, the right-hand side is reduced. Hence, by the uniqueness of reduced fraction expression, we must have $2 = a^2$ and $1 = b^2$. But this is impossible: 2 is not a perfect square. □

Irrational numbers

Theorem 8.10 (Irrationality of roots)

Let $\frac{a}{b}$ be a reduced fraction and n is an integer $\geqslant 2$. Then $\sqrt[n]{\frac{a}{b}}$ gives rational values if and only if both a and b are perfect n-th power (i.e. there are integers c, d such that $a = c^n$ and $b = d^n$.)

Irrational numbers

Theorem 8.10 (Irrationality of roots)

Let $\frac{a}{b}$ be a reduced fraction and n is an integer $\geqslant 2$. Then $\alpha =$ $\sqrt[n]{\frac{a}{b}}$ *gives rational values if and only if both a and b are perfect n-th power (i.e. there are integers c, d such that $a = c^n$ and $b = d^n$.)*

Proof. The "if" part is clear. Let's prove the "only if" part. Suppose our number α can be expressed as a reduced fraction $\frac{c}{d}$. Then

$$\frac{c^n}{d^n} = \left(\frac{c}{d}\right)^n = \alpha^n = \frac{a}{b}.$$

By the uniqueness of reduced fraction expression, we must have $a = c^n$ and $b = d^n$. $\square$

Another useful result is the following criterion:

Theorem 8.11 (Rational root theorem)

Let $\frac{a}{b}$ *be a reduced fraction expressing a root of a polynomial*

$$P(T) = c_n T^n + \cdots + c_1 T + c_0 \qquad (c_i \in \mathbb{Z}).$$

Then $a \mid c_0$ *and* $b \mid c_n$.

Theorem 8.11 (Rational root theorem)

Let $\frac{a}{b}$ be a reduced fraction expressing a root of a polynomial

$$P(T) = c_n T^n + \cdots + c_1 T + c_0 \qquad (c_i \in \mathbb{Z}).$$

Then $a \mid c_0$ and $b \mid c_n$.

Proof. Substitute $\frac{a}{b}$ into the polynomial,

$$c_n\left(\frac{a}{b}\right)^n + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

We thus have

$$c_n a^n + \underbrace{c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1}}_{\text{by } a \,\&\, b} + c_0 b^n = 0.$$

Then we must also have $a \mid c_0 b^n$ and $b \mid c_n a^n$. Since a, b are coprime, we have $a \mid c_0$ and $b \mid c_n$. □

Algebraic numbers

Algebraic numbers

Definition 8.12

A complex number α is ***algebraic*** if it is a root of a nonzero integer polynomial. Namely, there are integers $c_0, \cdots, c_n$ such that

$$c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0.$$

Otherwise, we say α is ***transcendental***.

Algebraic numbers

Definition 8.12

A complex number α is ***algebraic*** if it is a root of a nonzero integer polynomial. Namely, there are integers $c_0, \cdots, c_n$ such that

$$c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0.$$

Otherwise, we say α is ***transcendental***.

Example 8.13

Rational numbers are algebraic. Indeed, if $\frac{a}{b}$ is a fraction expressing our rational number α, then α is a root of $bT - a$.

Example 8.14

n-th roots of rationals are algebraic. Indeed $\sqrt[n]{\frac{a}{b}}$ is a root of $bT^n - a$.

Example 8.15

$2\sqrt{2} + \sqrt{3}$ is algebraic.

Proof. Let $\alpha = 2\sqrt{2} + \sqrt{3}$. We want to find an integer polynomial $P(T)$ such that $P(\alpha) = 0$.

$$\begin{aligned} \alpha &= 2\sqrt{2} + \sqrt{3} && \text{our definition} \\ \alpha - \sqrt{3} &= 2\sqrt{2} && \text{separate the roots} \\ \alpha^2 - 2\sqrt{3}\alpha + 3 &= 8 && \text{square both sides} \\ \alpha^2 - 5 &= 2\sqrt{3}\alpha && \text{separate the roots} \\ \alpha^4 - 10\alpha^2 + 25 &= 12\alpha^2 && \text{square both sides} \end{aligned}$$

1 get ride of root!

2 get ride of root!

Therefore, $\alpha^4 - 22\alpha^2 + 25 = 0$. Namely, α is a root of the integer polynomial $T^4 - 22T^2 + 25$. $\square$

Corollary 8.16

$2\sqrt{2}+\sqrt{3}$ *is irrational.*

Proof. Suppose for the sake of contradiction that $2\sqrt{2}+\sqrt{3}$ can be expressed by the reduced fraction $\frac{a}{b}$. Then since it is a root of integer polynomial $T^4 - 22T^2 + 25$, by the ***rational root theorem***, we must have $a \mid 25$ and $b \mid 1$. Therefore, the fraction $\frac{a}{b}$ can only be one of the following:

$$\pm 25, \pm 5, \pm 1.$$

Note that $2 < 2\sqrt{2} < 3$ since $4 < 8 < 9$, and that $1 < \sqrt{3} < 2$ since $1 < 3 < 4$. Thus, $3 < 2\sqrt{2}+\sqrt{3} < 5$. But none of above falls in this interval, which is a contradiction. $\square$

Alternatively, we can also just plug in $\pm 25, \pm 5, \pm 1$ into the polynomial.

After Class Work

Linear independence

Terminology

A $\mathbb{Q}$-***module*** is an abelian group $(M, +, e)$ together with an action of integers $\rho\colon \mathbb{Q} \times M \longrightarrow M$ satisfying

- (***associativity***) $\rho(ab, x) = \rho(a, \rho(b, x))$ for all $a, b \in \mathbb{Q}$ and $x \in M$;
- (***neutrality***) $\rho(a, e) = e$ for all $a \in \mathbb{Q}$.

Example 8.17

$(\mathbb{F}, +, 0)$ (where $\mathbb{F}$ is one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) is a $\mathbb{Q}$-module under the left multiplication.

The notion of $\mathbb{Q}$-***modules*** is very similar to ***vector spaces***. In fact, some authors may also call them $\mathbb{Q}$-***vector spaces***.

Linear independence

Terminology

Let $x_1, \cdots, x_n$ be elements in a $\mathbb{Q}$-module M. We say they are $\mathbb{Q}$***-linearly independent*** if the only $\mathbb{Q}$-linear combination

$$a_1 x_1 + \cdots + a_n x_n$$

of $x_1, \cdots, x_n$ expressing 0 is the ***trivial*** one: all coefficients $a_1, \cdots, a_n$ are 0.

Please compare this notion with ***linear independence*** in Linear Algebra course.

we need this is "1". otherwise thm is Not true

Theorem 8.18

$\alpha \in \mathbb{C}$ is irrational if and only if $1, \alpha$ are $\mathbb{Q}$-linearly independent.

Proof. ($\Longleftarrow$) If $\alpha \in \mathbb{Q}$, then $\alpha \cdot 1 + (-1) \cdot \alpha$ gives a non-trivial $\mathbb{Q}$-linear combination of $1, \alpha$ expressing 0.

($\Longrightarrow$) Suppose there are $\mathbb{Q}$-linear combination $a \cdot 1 + b \cdot \alpha$ is a non-trivial $\mathbb{Q}$-linear combination of $1, \alpha$ expressing 0. Then we must have $b \neq 0$, otherwise $a = a \cdot 1 + 0 \cdot \alpha = 0$ and hence this is a trivial combination. Then we have $\alpha = -\frac{a}{b}$. Hence, $\alpha \in \mathbb{Q}$. $\square$

$$a \cdot 1 + b \cdot \alpha = 0 \Rightarrow \alpha = \frac{-a \in \mathbb{Q}}{b \in \mathbb{Q}} = \frac{-\frac{a_1}{a_2}}{\frac{b_1}{b_2}} = -\frac{a_1 b_2}{a_2 b_1}$$

a fraction!