Rational numbers

March 9^{th}, 2021

Introduction

We want to enlarge $\mathbb{Z}$ with numbers of the form $\frac{p}{q}$, where $p \in \mathbb{Z}$ and $q \in \mathbb{Z} \setminus \{0\}$ satisfying the property that $\frac{p}{q} \times q = p$.
Such numbers are called rational numbers and they form the set $\mathbb{Q}$.
We also want to extend our operations $+, \times$ and the order $\leq$ from $\mathbb{Z}$ to $\mathbb{Q}$.

Set $x = \frac{10}{14}$ and $y = \frac{5}{7}$. Then $14x = 10$.
So, assuming the multiplication on $\mathbb{Q}$ has a cancellation rule, we get $7x = 5$, i.e. $x = \frac{5}{7} = y$.
Therefore, to have a coherent construction, we need to identify several fractions which are not equal *a priori*.

The usual formal way to achieve this point relies on *equivalence classes*, which is the point of view adopted in the lecture notes. I will adopt a more naive/less formal approach in the slides.

Definition

Definition

We define

$$\mathbb{Q} = \left\{ \frac{p}{q} \; : \; p \in \mathbb{Z},\, q \in \mathbb{Z} \setminus \{0\} \right\}$$

with the relation

$$\forall p, r \in \mathbb{Z},\, \forall q, s \in \mathbb{Z} \setminus \{0\},\, \frac{p}{q} = \frac{r}{s} \Leftrightarrow ps = qr$$

where the operation in the RHS takes place in $\mathbb{Z}$ (there is no cycling definition).

Example

$\frac{10}{14} = \frac{5}{7}$ since $10 \times 7 = 5 \times 14 = 70$.

A few notations

Notation

Note that the function $\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Q} \\ n & \mapsto & \frac{n}{1} \end{array}$ is injective.

Therefore we may see $\mathbb{Z}$ as a subset of $\mathbb{Q}$ by setting $n := \frac{n}{1} \in \mathbb{Q}$ for $n \in \mathbb{Z}$.

Notation

Note that for $(a,b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, we have $\frac{-a}{b} = \frac{a}{-b}$. Hence we set $-\frac{a}{b} := \frac{-a}{b} = \frac{a}{-b}$.

Notation

Note that $\frac{a}{b} = 0 \Leftrightarrow a = 0$ and that if $\frac{a}{b} = \frac{a'}{b'} \neq 0$ then $\frac{b}{a} = \frac{b'}{a'}$.

Hence, if $x = \frac{a}{b} \neq 0$, we set $x^{-1} := \frac{b}{a}$ which doesn't depend on the representative of x.

Lowest form representation

Proposition

Given $x \in \mathbb{Q}$, there exists a unique couple $(a, b) \in \mathbb{Z} \times \mathbb{N} \setminus \{0\}$ such that $x = \dfrac{a}{b}$ and $\gcd(a, b) = 1$.
Then we say that $x = \dfrac{a}{b}$ is written in *lowest form*.

Proof. Let $x \in \mathbb{Q}$.

Existence. There exist $\alpha \in \mathbb{Z}$ and $\beta \in \mathbb{Z} \setminus \{0\}$ such that $x = \frac{\alpha}{\beta}$.
Write $d = \gcd(\alpha, \beta)$, then there exist $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$ such that $\alpha = da$ and $\beta = db$.
Note that $\gcd(a, b) = 1$ (since $d = \gcd(\alpha, \beta) = \gcd(da, db) = d \gcd(a, b)$) and that $\frac{\alpha}{\beta} = \frac{\operatorname{sign}(b)a}{|b|}$ since $\operatorname{sign}(b)a\beta = \operatorname{sign}(b)adb = |b|da = |b|\alpha$.

Uniqueness. Assume that $\frac{a}{b} = \frac{a'}{b'}$ where $a, a' \in \mathbb{Z}$, $b, b' \in \mathbb{N} \setminus \{0\}$, $\gcd(a, b) = 1$, $\gcd(a', b') = 1$.
Then $ab' = a'b$. By Gauss' lemma, since $b|ab'$ and $\gcd(a, b) = 1$, we get that $b|b'$.
Similarly $b'|b$, so $|b| = |b'|$, thus $b = b'$.
Then, using the cancellation rule, $ab' = a'b$ gives $a = a'$ since $b = b' \neq 0$. ∎

Addition

Proposition

The addition $+ : \begin{array}{ccc} \mathbb{Q}\times\mathbb{Q} & \to & \mathbb{Q} \\ \left(\frac{a}{b},\frac{c}{d}\right) & \mapsto & \frac{ad+bc}{bd} \end{array}$ is well-defined.

Proof. We need to prove that the addition doesn't depend on the choice of the representatives, i.e. that if $\frac{a}{b}=\frac{a'}{b'}$ and $\frac{c}{d}=\frac{c'}{d'}$ then $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$.
Assume that $\frac{a}{b}=\frac{a'}{b'}$ and $\frac{c}{d}=\frac{c'}{d'}$, i.e. $ab'=ba'$ and $cd'=dc'$.
Therefore $(ad+bc)(b'd')=adb'd'+bcb'd'=ba'dd'+dc'bb'=(a'd'+b'c')(bd)$,
i.e. $\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$. ■

Remark

Note that the addition defined on $\mathbb{Q}$ is compatible with the one on $\mathbb{Z}$.
Indeed, if $m,n\in\mathbb{Z}$ then $\frac{m}{1}+\frac{n}{1}=\frac{m+n}{1}$.

Multiplication

Proposition

The multiplication $\times$: $\begin{array}{ccc} \mathbb{Q}\times\mathbb{Q} & \to & \mathbb{Q} \\ \left(\frac{a}{b},\frac{c}{d}\right) & \mapsto & \frac{ac}{bd} \end{array}$ is well-defined.

Proof. We need to prove that the multiplication doesn't depend on the choice of the representatives, i.e. that if $\frac{a}{b}=\frac{a'}{b'}$ and $\frac{c}{d}=\frac{c'}{d'}$ then $\frac{a}{b}\times\frac{c}{d}=\frac{a'}{b'}\times\frac{c'}{d'}$.

Assume that $\frac{a}{b}=\frac{a'}{b'}$ and $\frac{c}{d}=\frac{c'}{d'}$, i.e. $ab'=ba'$ and $cd'=dc'$.

Therefore $(ac)(b'd')=ab'cd'=ba'dc'=(a'c')(bd)$, i.e. $\frac{ac}{bd}=\frac{a'c'}{b'd'}$ as desired. ∎

Remark

Note that the multiplication defined on $\mathbb{Q}$ is compatible with the one on $\mathbb{Z}$.
Indeed, if $m,n\in\mathbb{Z}$ then $\frac{m}{1}\times\frac{n}{1}=\frac{m\times n}{1}$.

Order

We want to define an order on $\mathbb{Q}$, satisfying the following natural properties:

- $\frac{a}{b} \leq \frac{c}{d}$ if and only if $0 \leq \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$, and,
- $0 \leq \frac{e}{f}$ if and only if $0 \leq ef$ (i.e. the sign rule).

Therefore the following definition is natural:

Definition

We define the binary relation $\leq$ on $\mathbb{Q}$ by

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow 0 \leq (bc - ad)bd$$

where the order on the RHS of the equivalence is the order of $\mathbb{Z}$.

We have to check that it doesn't depend on the choice of the representative!

Proposition

The order $\leq$ defined on $\mathbb{Q}$ extends the usual order $\leq$ on $\mathbb{Z}$.

Proof. Let $m, n \in \mathbb{Z}$ then $\dfrac{m}{1} \leq \dfrac{n}{1} \Leftrightarrow 0 \leq n - m \Leftrightarrow m \leq n$. ∎

Properties

$(\mathbb{Q}, +, \times, \leq)$ is a (totally) ordered field, meaning that

- $+$ is associative: $\forall x, y, z \in \mathbb{Q},\ (x+y)+z = x+(y+z)$
- 0 is the unit of $+$: $\forall x \in \mathbb{Q},\ x+0 = 0+x = x$
- $-x$ is the additive inverse of x: $\forall x \in \mathbb{Q},\ x+(-x) = (-x)+x = 0$
- $+$ is commutative: $\forall x, y \in \mathbb{Q},\ x+y = y+x$
- $\times$ is associative: $\forall x, y, z \in \mathbb{Q},\ (xy)z = x(yz)$
- $\times$ is distributive with respect to $+$: $\forall x, y, z \in \mathbb{Q},\ x(y+z) = xy+xz$ and $(x+y)z = xz+yz$
- 1 is the unit of $\times$: $\forall x \in \mathbb{Q},\ 1 \times x = x \times 1 = x$
- If $x \neq 0$ then x^{-1} is the multiplicative inverse of x: $\forall x \in \mathbb{Q} \setminus \{0\},\ xx^{-1} = x^{-1}x = 1$
- $\times$ is commutative: $\forall x, y \in \mathbb{Q},\ xy = yx$
- $\leq$ is reflexive: $\forall x \in \mathbb{Q},\ x \leq x$
- $\leq$ is antisymmetric: $\forall x, y \in \mathbb{Q},\ \left(x \leq y \text{ and } y \leq x\right) \implies x = y$
- $\leq$ is transitive: $\forall x, y, z \in \mathbb{Q},\ \left(x \leq y \text{ and } y \leq z\right) \implies x \leq z$
- $\leq$ is total: $\forall x, y \in \mathbb{Q},\ x \leq y$ or $y \leq x$
- $\forall x, y, r, s \in \mathbb{Q},\ (x \leq y \text{ and } r \leq s) \Rightarrow x+r \leq y+s$
- $\forall x, y, z \in \mathbb{Q},\ \left(x \leq y \text{ and } z > 0\right) \Rightarrow xz \leq yz$

Between two rationals there is another rational

Proposition

$\forall x, y \in \mathbb{Q},\ x < y \implies (\exists z \in \mathbb{Q},\ x < z < y)$

Proof. Let $x, y \in \mathbb{Q}$ be such that $x < y$. Then $z = \frac{x+y}{2}$ is a suitable choice.
Indeed, $x < y$ implies $2x < x + y$ and thus $x < z$. Similarly $x + y < 2y$, and thus $z < y$. ∎

Remark

Note that $\mathbb{Q}$ is not well-ordered.
Indeed $\mathbb{Q}_{>0} = \{x \in \mathbb{Q}\ :\ x > 0\}$ is non-empty (and even bounded from below) but it has no least element.

Theorem: $\mathbb{Q}$ is archimedean

$\forall \varepsilon \in \mathbb{Q}_{>0}, \forall A \in \mathbb{Q}_{>0}, \exists N \in \mathbb{N}, N\varepsilon > A.$

Proof.
Since $\frac{A}{\varepsilon} > 0$, we may find a representative $\frac{a}{b} = \frac{A}{\varepsilon}$ where $a, b \in \mathbb{N} \setminus \{0\}$.
Then $a + 1 - \frac{A}{\varepsilon} = a + 1 - \frac{a}{b} = \frac{a(b-1)+b}{b} > 0$, thus $(a+1)\varepsilon > A$.
So $N = a + 1$ is a suitable choice. ∎

Remark

The above theorem means that $\lim\limits_{n \to +\infty} \frac{1}{n} = 0$, or equivalently that $\mathbb{Q}$ doesn't contain infinitesimal elements (i.e. there is not infinitely large or infinitely small elements).

The rational root theorem

The rational root theorem

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients $a_k \in \mathbb{Z}$.
If $x = \frac{p}{q}$ is a rational root of f written in lowest terms (i.e. $\gcd(p,q) = 1$), then $p|a_0$ and $q|a_n$.

Proof. By assumption we have that

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

Therefore

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

Thus $p|a_0 q^n$. Since $\gcd(p,q) = 1$, by Gauss' lemma we obtain that $p|a_0$.
Similarly $q|a_n$. ∎