Chapter 3

The Field $\mathbb{Q}$ of Rational Numbers

In this chapter we are going to construct the rational number from the integers. Historically, the positive rational numbers came first: the Babylonians, Egyptians and Greeks knew how to work with fractions, but negative numbers were introduced by the Hindus hundreds of years later. It is possible to reflect this in the build-up of the rationals from the natural numbers by first constructing the positive rational numbers from the naturals, and then introducing negatives (Landau proceeds like this in his Foundations of Analysis). While being closer to history, this has the disadvantage of getting a ring structure only at the end.

3.1 The Rational Numbers

Let $\mathbb{Z}$ denote the ring of integers and consider the set

$$V = \{(r, s) : r, s \in \mathbb{Z},\ s \neq 0\}$$

of pairs of integers. Let us define an equivalence relation on V by putting

$$(r, s) \sim (t, u) \iff ru = st.$$

It is easily seen that this is an equivalence relation, and we now let

$$[r, s] = \{(x, y) \in V : (x, y) \sim (r, s)\}$$

denote the equivalence class of (r, s).

Such an equivalence class $[r, s]$ is called a rational number, and we often write $\frac{r}{s}$ instead of $[r, s]$. We denote by $\mathbb{Q}$ the set of all equivalence classes $[r, s]$ with $(r, s) \in V$.

We start studying $\mathbb{Q}$ by realizing $\mathbb{Z}$ as a subset of $\mathbb{Q}$ via the map $\iota : \mathbb{Z} \longrightarrow \mathbb{Q}$ defined by $\iota(r) = [r, 1]$. Then ι is injective; in fact, assume that $x, y \in \mathbb{Z}$ are

such that $\iota(x) = \iota(y)$. Then $[x, 1] = [y, 1]$, i.e., $(x, 1) \sim (y, 1)$, and by definition of equivalence in V this means $x \cdot 1 = y \cdot 1$, hence $x = y$.

We want to have $\frac{r}{s} + \frac{t}{u} = \frac{ru+st}{su}$, so we are led to define

$$[r, s] \oplus [t, u] = [ru + st, su] \tag{3.1}$$

for $r, s, t, u \in \mathbb{Z}$ with $s, u > 0$. This is well defined and agrees with addition on $\mathbb{Z}$ under the identification ι: in fact,

$$\begin{aligned} \iota(x) \oplus \iota(y) &= [x, 1] \oplus [y, 1] \\ &= [x \cdot 1 + 1 \cdot y, 1 \cdot 1] = [x + y, 1] \\ &= \iota(x + y). \end{aligned}$$

Thus it does not matter whether we add in $\mathbb{Z}$ and then identify the result with a rational number, or first view the integers as elements of $\mathbb{Q}$ and add there.

Next we define multiplication of fractions by

$$[r, s] \odot [t, u] = [rt, su]. \tag{3.2}$$

This is motivated by $\frac{r}{s} \cdot \frac{t}{u} = \frac{rt}{su}$. Again, multiplication is well defined and agrees with multiplication on the subset $\mathbb{Z} \subset \mathbb{Q}$: we have $\iota(x) \odot \iota(y) = \iota(xy)$ because

$$\begin{aligned} \iota(x) \odot \iota(y) &= [x, 1] \odot [y, 1] && \text{by definition of } \iota \\ &= [xy, 1] && \text{by definition (3.2)} \\ &= \iota(xy) && \text{by definition of } \iota \end{aligned}$$

Remark. The map $\iota : \mathbb{Z} \longrightarrow \mathbb{Q}$ from the ring $\mathbb{Z}$ to the ring of fractions $\mathbb{Q}$ satisfies

$$\begin{aligned} \iota(x) \oplus \iota(y) &= \iota(x + y), \\ \iota(x) \odot \iota(y) &= \iota(xy), \end{aligned}$$

Maps $R \longrightarrow S$ between rings with these properties (we say that they 'respect the ring structure') are called ring homomorphisms if they map the unit element of R to the unit element of S. In particular, our 'identification map' ι is a ring homomorphism.

Using these definitions, we can prove associativity, commutativity, distributivity, thereby verifying that $\mathbb{Q}$ is a ring. In fact, $\mathbb{Q}$ is even a field!

A field F is a commutative ring in which, informally speaking. we can divide by nonzero elements: thus F is a field if F satsifies the ring axioms (in particular we have $1 \neq 0$), and if in addition

F1 For every $r \in F \setminus \{0\}$ there is an $s \in F$ such that $rs = 1$.

Observe that F1 holds if and only if $F^\times = F \setminus \{0\}$.

This is a strong axiom: together with some other ring axioms it implies that fields are integral domains:

Proposition 3.1. *If F is a field and if $xy = 0$ for $x, y \in F$, then $x = 0$ or $y = 0$.*

Proof. In fact, assume that $xy = 0$ and $y \neq 0$. Since the nonzero elements of F form a group, y has an inverse, that is, there is a $z \in F$ such that $yz = 1$. But now $0 = xy$ implies $0 = 0z = (xy)z = x(yz) = x \cdot 1 = x$; here we have used associativity of multiplication. □

We have proved

Theorem 3.2. *The set $\mathbb{Q}$ of rational numbers forms a field with respect to addition and multiplication.*

We can also define powers of rational numbers: if $a \in \mathbb{Q}$ is nonzero, we put $a^0 = 1$ and $a^{n+1} = a^n \cdot a$. This defines a^n for all $n \in \mathbb{N}$; if n is negative, we put $a^n = 1/a^{-n}$.

We now can prove the well known set of rules $a^n a^m = a^{n+m}$, $a^{mn} = (a^m)^n$, $a^n b^n = (ab)^n$ etc.

Binomial Theorem

The next result is called the Binomial Theorem. Before we can state it, we have to introduce the binomial coefficients. These are defined in terms of factorials, so we have to define these first. To this end, we put $0! = 1$ and $(n+1)! = n! \cdot (n+1)$ for $n \in \mathbb{N}$. Now we set $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ for $0 \leq k \leq n$ and $\binom{n}{k} = 0$ if $k < 0$ or $k > n$.

Lemma 3.3. *The binomial coefficients are integers. In fact, we have $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ for $n \geq 0$ and $k \geq -1$.*

Proof. This is a simple computation:

$$\begin{aligned} \binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k-1)!}\Big\{\frac{1}{n-k} + \frac{1}{k+1}\Big\} \\ &= \frac{n!}{k!(n-k-1)!}\frac{n+1}{(n-k)(k+1)} = \binom{n+1}{k+1}. \end{aligned}$$

This calculation is valid for $k \geq 0$; for $k = -1$, we have $\binom{n}{k} = 0$, $\binom{n}{k+1} = 1 = \binom{n+1}{k+1}$, and the claim holds. □

Now we have

Theorem 3.4 (Binomial Theorem)**.** *For $a, b \in \mathbb{Q}^\times$ and $n \in \mathbb{N}$, we have*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Proof. This is done by induction on n. For $n = 1$, we have to prove $(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k} = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1$, which is true since $\binom{1}{0} = \binom{1}{1} = 1$.

Now assume that the claim holds for some integer $n \geq 1$; then

$$\begin{aligned}
(a+b)^{n+1} = (a+b)^n (a+b) &= \Big(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \Big)(a+b) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{l=1}^{n+1} \binom{n}{l-1} a^{n+1-l} b^l \\
&= \binom{n}{0} a^{n+1} + \sum_{k=1}^{n} \Big(\binom{n}{k} + \binom{n}{k-1} \Big) a^{n+1-k} b^k + \binom{n}{n} b^{n+1} \\
&= \binom{n+1}{0} a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k + \binom{n+1}{n+1} b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k,
\end{aligned}$$

which is exactly what we wanted to prove. □

3.2 $\mathbb{Q}$ as an ordered field

Observe that every rational number can be written as $[r, s]$ with $s \geq 1$ (if $s \leq -1$, recall that $[r, s] = [-r, -s]$). From now on, we will assume that all our rational numbers are presented like this. We define an order relation $<$ on $\mathbb{Q}$ by putting

$$[r, s] < [t, u] \iff ru < st$$

(recall that $s, u \in \mathbb{N}$). This is well defined: if $[r, s] = [r', s']$ and $[t, u] = [t', u']$, then $rs' = r's$ and $tu' = t'u$. Now

$$\begin{array}{lcll}
[r, s] < [t, u] & \iff & ru < st & \text{by definition} \\
& \iff & rus'u' < sts'u' & \text{since } s'u' > 0 \\
& \iff & r'suu' < ss't'u & \text{since } rs' = r's \text{ and } tu' = t'u \\
& \iff & r'u' < s't' & \text{since } su > 0 \\
& \iff & [r', s'] < [t', u'] & \text{by definition}
\end{array}$$

Now we have

Theorem 3.5. *$\mathbb{Q}$ is an ordered domain (even field).*

Proof. Since exactly one of the relations $ru < st$, $ru = st$ or $ru > st$ is true by the trichotomy law for integers, exactly one of $x < y$, $x = y$ or $x > y$ is true for $x = [r, s]$ and $y = [t, u]$.

Next assume that $x < y$ and $y < z$, where $z = [v, w]$. Then $ru < st$ and $tw < uv$, hence $ruw < stw$ and $stw < suv$ since $w, s > 0$; transitivity for the integers gives $ruw < suv$, and since $u > 0$, this is equivalent to $rw < sv$, i.e., $x < z$.

This shows that $\mathbb{Q}$ is simply ordered. The rest of the proof that $\mathbb{Q}$ is an ordered domain is left as an exercise. □

Thus everything proved for general ordered domains holds for the rationals; in particular, $x^2 \geq 0$ for all $x \in \mathbb{Q}$, and $|x + y| \leq |x| + |y|$ for $x, y \in \mathbb{Q}$.

Now let us collect a few simple results that will turn out to be useful.

Lemma 3.6. *We have $|x| < |y|$ if and only if $n|x| < n|y|$ for some $n \in \mathbb{N}$.*

Proof. Exercise. □

Proposition 3.7. *Let $x, y \in \mathbb{Q}$ and assume that for every rational $\varepsilon > 0$ we have $|x - y| < \varepsilon$; then $x = y$.*

Proof. Assume that this is false, i.e. that $x - y \neq 0$. Then $\varepsilon = |x - y|$ is a positive rational number, so by assumption we have $|x - y| < \varepsilon$. This implies $\varepsilon < \varepsilon$, which is a contradiction. □

Proposition 3.8. *Let $0 < x < y$ be rational numbers. Then there is an $n \in \mathbb{N}$ such that $nx > y$.*

Proof. Write $x = \frac{r}{s}$ and $y = \frac{s}{t}$ with $r, s, t, u \in \mathbb{N}$ (here we have used that $x, y > 0$). Then $x < y$ is equivalent to $ru < st$; by the Archimedean property of the natural numbers there is an $n \in N$ such that $n(ru) > st$. But the last inequality is equivalent to $nx > y$. □

Division with remainder in $\mathbb{Z}$ allows us to introduce the floor function in $\mathbb{Q}$: for rational numbers $x = \frac{a}{b}$ with $b > 0$, we put $\lfloor x \rfloor = q$ if $a = bq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < b$. Note that this is well defined: if $x = \frac{c}{d}$ with $d > 0$, $c = dq' + r'$ and $0 \leq r' < d$, then $ad = bc$, hence $ad = bdq + rd$, $bc = bdq' + br'$, and therefore $0 = bd(q - q') + rd - r'b$. We may assume without loss of generality that $q \geq q'$; if $q \neq q'$, then $q \geq q' + 1$, hence $bd > r'b = bd(q - q') + rd \geq bd + rd \geq bd$: contradiction.

Proposition 3.9. *For $x \in \mathbb{Q}$, the integer $\lfloor x \rfloor$ is the unique integer satisfying $x - 1 < \lfloor x \rfloor \leq x$.*

Proof. First, there is exactly one integer m satisfying $x - 1 < m \leq x$ because $|m - n| < 1$ for integers implies $|m - n| = 0$, hence $m = n$. It is therefore sufficient to prove that $x - 1 < \lfloor x \rfloor \leq x$.

To this end, recall that $q = \lfloor x \rfloor$ is defined for $x = \frac{a}{b}$ by $0 \leq a - bq < b$. Dividing through by $-b$ and adding x we get $x - 1 < q \leq x$ as claimed. □

For any rational number x, we call $\langle x \rangle = x - \lfloor x \rfloor$ the fractional part of x. Note that $0 \leq \langle x \rangle < 1$ for all rational numbers $x \in \mathbb{Q}$.

3.3 Irrational Numbers

The irrationality of 2, at least in its geometric form (the side and the diagonal of a square are incommensurable) seems to have been discovered by the Pythagoreans. Although by the time of Euclid it was known that square roots of nonsquares are irrational, Euclid's elements only contain the proof that $\sqrt{2}$ is not rational; in this case, a proof can be given depending only on the 'theory of the odd and the even', as the Greeks called the most elementary parts of number theory.

Theorem 3.10. *If $n \in \mathbb{N}$ is not the square of an integer, then it is not the square of a rational number.*

Proof 1. In fact, if n is not a square of an integer, then it lies between two squares, that is, we can find an integer a such that $a^2 < n < (a+1)^2$. Assume that $\sqrt{n} = \frac{p}{q}$ with $q > 0$ minimal. Then $p^2 = nq^2$, hence $p(p-aq) = p^2 - apq = nq^2 - apq = q(nq - ap)$, so

$$\frac{p}{q} = \frac{nq - ap}{p - aq}.$$

But $a < \frac{p}{q} < a + 1$ implies $0 < p - aq < q$: this contradicts the minimality of the denominator q. □

Proof 2. [1] Assume that $n = A/B$ with $B > 0$ minimal; then $A/B = nB/A$, hence both of these fractions have the same fractional part, say $b/B = \langle A/B \rangle = \langle nB/A \rangle = a/A$ with $0 < a < A$ and $0 < b < B$ (note that e.g. $a = 0$ would imply that n is an integer). But then $A/B = a/b$, and $0 < b < B$ contradicts the minimality of $B > 0$. □

Proof 3. Since n is not a square, at least one prime p divides n to an odd power. If we had $\sqrt{n} = \frac{b}{a}$, squaring and clearing denominators would give $b^2 n = a^2$, and p would divide a^2 to an odd power, contradicting unique factorization. □

3.4 Historical Remarks

Long before mankind discovered 0 and the negative numbers, they started working with positive rational numbers. The Babylonians had sexagesimal fractions, and the Egyptians essentially worked with pure fractions, that is, those that can be written in the form $\frac{1}{n}$. Every fraction was represented by a sum of *different* pure fractions: for example, they would have written $\frac{2}{5}$ not as $\frac{1}{5} + \frac{1}{5}$, but as $\frac{2}{5} = \frac{1}{3} + \frac{1}{15}$.

Fractions were not regarded as numbers in Euclid's elements; Eudoxos' theory of proportions dealt with magnitudes, that is, 'lengths' and 'areas' etc. Archimedes and Diophantus, on the other hand, worked freely with positive rational numbers.

[1] Due to John Conway.

Exercises

3.1 For $a, b \in \mathbb{Q}$, we have

$$a \leq \frac{a+b}{2} \leq b.$$

The rational number $\frac{a+b}{2}$ is called the arithmetic mean of a and b.

3.2 For $a, b \in \mathbb{Q}^\times$, we have

$$a \leq \frac{2}{\frac{1}{a} + \frac{1}{b}} \leq b.$$

The rational number $\frac{2}{\frac{1}{a}+\frac{1}{b}}$ is called the harmonic mean of a and b.

3.3 Prove that for all $a, b \in \mathbb{Q}^\times$, we have

$$\frac{2}{\frac{1}{a} + \frac{1}{b}} \leq \frac{a+b}{2}.$$

This is called the inequality between harmonic and arithmetic mean. Show that equality holds if and only if $a = b$.

3.4 Which of the proofs of the irrationality of $\sqrt{n}$ for nonsquares n generalizes to m-th roots of integers?