Lecture 2: Functions and Rational Numbers

2.1 Functions

If A and B are sets, a relation $R \subset A \times B$ is called a *function* with *domain* A if for every $a \in A$ there exists one, and only one, $b \in B$ such that $(a, b) \in R$. We typically indicate such a relation with the notation $f : A \to B$, and write $f(a) = b$ to indicate that $(a, b) \in R$. The set of all $b \in B$ such that $f(a) = b$ for some $a \in A$ is called the *range* of f.

We say $f : A \to B$ is *one-to-one* if for every b in the range of f there exists a unique $a \in A$ such that $f(a) = b$. We say f is *onto* if for every $b \in B$ there exists at least one $a \in A$ such that $f(a) = b$. For example, the function $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f(z) = z^2$ is one-to-one, but not onto, whereas the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(z) = z + 1$ is both one-to-one and onto.

Given two functions, $f : A \to B$ and $g : B \to C$, we define the *composition*, denoted $f \circ g : A \to C$, to be the function defined by $f \circ g(a) = f(g(a))$.

If $f : A \to B$ is both one-to-one and onto, then we may define a function $f^{-1} : B \to A$ by requiring $f^{-1}(b) = a$ if and only if $f(a) = b$. Note that his implies that $f \circ f^{-1}(b) = b$ for all $b \in B$ and $f^{-1} \circ f(a) = a$ for all $a \in A$. We call f^{-1} the *inverse* of f.

Given any collection of nonempty sets, $\{A_\alpha\}$, $\alpha \in I$, we assume the existence of a function $\phi : I \to B$, $B = \bigcup_{\alpha \in I} A_\alpha$, with the property that $\phi(\alpha) \in A_\alpha$. Such a function is called a *choice function* and the assumption that choice functions always exist is known as the *Axiom of Choice*.

2.2 Rational numbers: field properties

Let $P = \{(p, q) : p, q \in \mathbb{Z}, q \neq 0\}$. We define an equivalence relation on P by saying $(p, q) \sim (s, t)$ if $pt = qs$.

Exercise 2.2.1
Show that the relation as just defined is indeed an equivalence relation.

We will denote the equivalence class of $(p, q) \in P$ by p/q, or $\frac{p}{q}$. The set of all equivalence classes of P is called the *rational numbers*, which we denote by $\mathbb{Q}$. If $p \in \mathbb{Z}$, we will denote the equivalence class of $(p, 1)$ by p; that is, we let

$$\frac{p}{1} = p.$$

In this way, we may think of $\mathbb{Z}$ as a subset of $\mathbb{Q}$.

We wish to define operations of addition and multiplication on elements of $\mathbb{Q}$. We begin by defining operations on the elements of P. Namely, given $(p, q) \in P$ and $(s, t) \in P$, define

$$(p, q) \oplus (s, t) = (pt + sq, qt)$$

and

$$(p, q) \otimes (s, t) = (ps, qt).$$

Now suppose $(p, q) \sim (a, b)$ and $(s, t) \sim (c, d)$. It follows that $(p, q) \oplus (s, t) \sim (a, b) \oplus (c, d)$, that is, $(pt + sq, qt) \sim (ad + cb, bd)$, since

$$(pt + sq)bd = pbtd + sdqb = qatd + tcqb = (ad + cb)qt.$$

Moreover, $(p,q) \otimes (s,t) \sim (a,b) \times (c,d)$, that is, $(ps,qt) \sim (ac,bd)$, since

$$psbd = pbsd = qatc = qtac.$$

This shows that the equivalence class of a sum or product depends only on the equivalence classes of the elements being added or multiplied. Thus we may define addition and multiplication on $\mathbb{Q}$ by

$$\frac{p}{q} + \frac{s}{t} = \frac{pt + sq}{qt}$$

and

$$\frac{p}{q} \times \frac{s}{t} = \frac{ps}{qt},$$

and the results will not depend on which representatives we choose for each equivalence class. Of course, multiplication is often denoted using juxtaposition, that is,

$$\frac{p}{q} \times \frac{s}{t} = \frac{p}{q}\frac{s}{t},$$

and repeated multiplication may be denoted by exponentiation, that is, a^n, $a \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$, represents the product of a with itself n times.

Note that if $(p,q) \in P$, then $(-p,q) \sim (p,-q)$. Hence, if $a = \frac{p}{q} \in \mathbb{Q}$, then we let

$$-a = \frac{-p}{q} = \frac{p}{-q}.$$

For any $a, b \in \mathbb{Q}$, we will write $a - b$ to denote $a + (-b)$.

If $a = \frac{p}{q} \in \mathbb{Q}$ with $p \neq 0$, then we let

$$a^{-1} = \frac{q}{p}.$$

Moreover, we will write

$$\frac{1}{a} = a^{-1},$$

$$\frac{1}{a^n} = a^{-n}$$

for any $n \in \mathbb{Z}^+$, and, for any $b \in \mathbb{Q}$,

$$\frac{b}{a} = ba^{-1}.$$

It is now easy to show that

(1) $a + b = b + a$ for all $a, b \in \mathbb{Q}$;
(2) $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Q}$;
(3) $ab = ba$ for all $a, b \in \mathbb{Q}$;
(4) $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{Q}$;

(5) $a(b+c) = ab + ac$ for all $a, b, c \in \mathbb{Q}$;
(6) $a + 0 = a$ for all $a \in \mathbb{Q}$;
(7) $a + (-a) = 0$ for all $a \in \mathbb{Q}$;
(8) $1a = a$ for all $a \in \mathbb{Q}$;
(9) if $a \in \mathbb{Q}$, $a \neq 0$, then $aa^{-1} = 1$.

Taken together, these statements imply that $\mathbb{Q}$ is a *field.*

2.3 Rational numbers: order and metric properties

We say a rational number a is *positive* if there exist $p, q \in \mathbb{Z}^+$ such that $a = \frac{p}{q}$. We denote the set of all positive elements of $\mathbb{Q}$ by $\mathbb{Q}^+$.

Given $a, b \in \mathbb{Q}$, we say a is *less than* b, or, equivalently, b is *greater than* a, denoted either by $a < b$ or $b > a$, if $b - a$ is positive. In particular, $a > 0$ if and only if a is positive. If $a < 0$, we say a is *negative.* We write $a \leq b$, or, equivalently, $b \geq a$ if either $a < b$ or $a = b$.

Exercise 2.3.1
Show that for any $a \in \mathbb{Q}$, one and only one of the following must hold: (a) $a < 0$, (b) $a = 0$, (c) $a > 0$.

Exercise 2.3.2
Show that if $a, b \in \mathbb{Q}^+$, then $a + b \in \mathbb{Q}^+$.

Exercise 2.3.3
(a) Show that for any $a, b \in \mathbb{Q}$, one and only one of the following must hold: (a) $a < b$, (b) $a = b$, (c) $a > b$.
(b) Show that if $a, b, c \in \mathbb{Q}$ with $a < b$ and $b < c$, then $a < c$.
(c) Show that if $a, b, c \in \mathbb{Q}$ with $a < b$, then $a + c < b + c$.
(d) Show that if $a, b \in \mathbb{Q}$ with $a > 0$ and $b > 0$, then $ab > 0$.

As a consequence of Exercise 2.3.3, we say $\mathbb{Q}$ is an *ordered field.*

Exercise 2.3.4
Show that if $a, b \in \mathbb{Q}$ with $a > 0$ and $b < 0$, then $ab < 0$.

Exercise 2.3.5
Show that if $a, b, c \in \mathbb{Q}$ with $a < b$, then $ac < bc$ if $c > 0$ and $ac > bc$ if $c < 0$.

Exercise 2.3.6
Show that if $a, b \in \mathbb{Q}$ with $a < b$, then $a < \frac{a+b}{2} < b$.

For any $a \in \mathbb{Q}$, we call

$$|a| = \begin{cases} a, & \text{if } a \geq 0, \\ -a, & \text{if } a < 0, \end{cases}$$

the *absolute value* of a.

Exercise 2.3.7
Show that for any $a \in \mathbb{Q}$, $-|a| \leq a \leq |a|$.

Proposition For any $a, b \in \mathbb{Q}$, $|a + b| \leq |a| + |b|$.

Proof If $a+b \geq 0$, then

$$|a|+|b|-|a+b|=|a|+|b|-a-b=(|a|-a)+(|b|-b).$$

Both of the terms on the right are nonnegative by Exercise 2.3.7. Hence the sum is nonnegative and the proposition follows. If $a+b<0$, then

$$|a|+|b|-|a+b|=|a|+|b|+a+b=(|a|+a)+(|b|+b).$$

Again, both of the terms on the right are nonnegative by Exercise 2.3.7. Hence the sum is nonegatvie and the proposition follows.

It is now easy to show that the absolute value satisfies

(1) $|a-b| \geq 0$ for all $a, b \in \mathbb{Q}$, with $|a-b|=0$ if and only if $a=b$,
(2) $|a-b|=|b-a|$ for all $a, b \in \mathbb{Q}$,
(3) $|a-b| \leq |a-c|+|c-b|$ for all $a, b, c \in \mathbb{Q}$.

Note that the last statement, known as the *triangle inequality*, follows from writing

$$a-b=(a-c)+(c-b)$$

and applying the previous proposition. These properties show that the function

$$d(a, b)=|a-b|$$

is a *metric*, and we will call $|a-b|$ the *distance* from a to b.

Suppose $a, b \in \mathbb{Q}^{+}$ with $a<b$ and let $p, q, r, s \in \mathbb{Z}^{+}$ such that $a=\frac{p}{q}$ and $b=\frac{r}{s}$. For any $n \in \mathbb{Z}^{+}$, we have

$$na-b=n\frac{p}{q}-\frac{r}{s}=\frac{nps-rq}{qs}.$$

If we choose n large enough so that $nps-rq>0$, it follows that $na-b>0$, that is, $na>b$. We say that the ordered field $\mathbb{Q}$ is *archimedean*. Note that it also follows that we may choose n large enough to ensure that $\frac{b}{n}<a$.