Rational Numbers

- There are four standard arithmetic operations: addition, subtraction, multiplication, and division.
- Just as we took differences of natural numbers to represent integers, here the essence of the process is to use ordered pairs representing quotients.
- (2,3), (8,12), (-50, -75), and (1000, 1500) will all represent the same object.

Definition: Let a,c $\in \mathbb{Z}$, and let b, d $\in \mathbb{Z}$ /{0}. We say that (a, b) is related to (c,d), written (a,b) # (c,d) if ad = bc.

- Intuition: This expresses what we would like a/b = c/d (a, b) # (c,d) if a/b and c/d represent the same natural number. ad = bc.

Proposition: # is an equivalence relation.

Proof: Reflexive Property

For any a,b $\in \mathbb{Z}$ with b $\neq$ 0
ab = ab, so (a,b) # (a,b)

Symmetric Property –

Suppose that (a,b) # (c,d) so that ad = bc
cb = da so by the commutivity of $\mathbb{Z}$
(c,d) # (a,b)

Transitive Property –

Suppose that (a,b) # (c,d) and (c,d) # (e,f)
where a,c,e $\in \mathbb{Z}$ and b,d,f $\in \mathbb{Z}$ /{0}
Then ad = bc and cf = de and thus
afd = adf = bcf = bde = bed
Since d $\neq$ 0 we can deduce af = be by cancellation of $\mathbb{Z}$,
af = be and thus (a,b) # (e,f)

■

- Define the set of rational numbers to be the set of equivalence classes under #.

Example:

The set {(a, b): a, b $\in \mathbb{Z}$, b$\neq$0, b = 2a} is an equivalence class. (The class determined by (1,2).)

- Let us denote the equivalence class determined by (a, b) by a/b. What we intend is that a/b should be the rational number that we intuitively think of as a/b.
- This construction of the rationals is modeled on that of the integers so as to emphasize the analogy. The construction of the integers involved introducing ‘additive inverses’ for the natural numbers, and now the construction of the rational numbers involves the introduction of ‘multiplicative inverses’ for the non-zero integers. We must also introduce other new objects; besides requiring rational numbers of the form 1/b (b$\in \mathbb{Z}$, b$\neq$0) we also have rations of the form a/b which cannot be reduced (by cancellation) to a fraction with numerator 1.
- So far we have only a set. Now we must describe the operations of addition, multiplication, subtraction, and division, to investigate the natural order of the

rational numbers, and to examine the way in which the newly defined set of rational numbers contains the set of integers.

Definition: Addition and Multiplication of rational numbers are defined as follows. Let $a, b, c, d \in \mathbb{Z}$, with $b \neq 0$, $d \neq 0$.

$a/b + c/d = (ad+bc)/bd$
$a/b * c/d = ac/bd$

Some properties of rational numbers –

Proposition: Multiplication in the rational numbers is well-defined.

Proof: Suppose that $a/b = p/q$ and $c/d – r/s$.
Show that $ac/bd = pr/qs$ ($(ac, bd) \# (pr, qs)$, $acqs = bdpr$)
$a/b = p/q$ thus $aq = bp$ and $c/d = r/s$ thus $cs = dr$
$acqs = bdpr$
$(ac, bd) \# (pr, qs)$
$ac/bd = pr/qs$

■

Proposition: Addition in the rational numbers is well-defined.

Proof: Left to the reader

- If a/b is a rational number, and x is a non-zero integer, then $ax/bx = a/b$. ($axb = bxa$ and thus $(ax, bx) \# (a, b)$)

Proposition: Addition and Multiplication of rational numbers are commutative and associative, and the distributive law holds.

Proof: These results are easy consequences of the corresponding properties of integers.

Proposition: There are rational numbers that behave like zero and one. For any $a, b \in \mathbb{Z}$, with $b \neq 0$, we have: $a/b + 0/1 = a/b$, $a/b * 1/1 = a/b$, $a/b * 0/1 = 0/1$.

Proof: Proofs incorporate the definitions and properties of natural numbers.

- Thus $0/1$ behaves like zero in the natural numbers, $1/1$ behaves like one, and for any non-zero b, $b/b = 1/1$.

Proposition: For any $a, b \in \mathbb{Z}/\{0\}$, we have $a/b * b/a = ab/ab = 1/1$.

Proof: Also follows from the definition of multiplication.

- Thus b/a is a multiplicative inverse of a/b, this enables us to introduce the operation of division. Division by a/b in the rationals is defined to be the same as multiplying by b/a (if and only if $a \neq 0$). Thus we can only divide by non-zero numbers.
- Additive inverses are straightforward. For $a, b \in \mathbb{Z}$, with $b \neq 0$ we have $a/b \pm (-a)/b = (ab – ab)/b^2 = 0/b^2 = 0/1$. Hence we may write $–(a/b)$ for $(-a)/b$. Observe that $(-a)/b = a/(-b)$.

- Subtraction: For $a, b, c, d \in \mathbb{Z}$, with $b \neq 0$, $d \neq 0$, let $a/b - c/d$ stand for $a/b + (-(c/d))$.
- We denote the set of rational numbers by $\mathbb{Q}$.
- From the above, it can be shown that the set of rationals for a field uner '+' and '*'.

Definition: The <u>order relation</u> on $\mathbb{Q}$ is defined as follows. We say that an element a/b of $\mathbb{Q}$ is positive if $ab > 0$, where ab is an integer.

Proposition: Order relation on $\mathbb{Q}$ is well defined.

Proof: Suppose that $a/b = c/d$ and a/b is positive.
Then $ad = bc$ and $ab > 0$. It follows that
$cdb^2 = bcbd = adbd = abd^2$.
Since $b^2 > 0$, $d^2 > 0$ and $ab > 0$, we must have $cd > 0$.

■

Definition: Let $\mathbb{Q}^+$ denote the set of positive rational numbers. Now define $<$ on $\mathbb{Q}$ by :

$x < y$ if $y-x \in \mathbb{Q}^+$.

- The definition of $\leq$ is now just as one would expect.

Theorem:

1. Given $x \in \mathbb{Q}$, one of the following holds:
   $x \in \mathbb{Q}^+$
   $x = 0$
   $-x \in \mathbb{Q}^+$
2. If $x, y \in \mathbb{Q}^+$, then $x + y \in \mathbb{Q}^+$ and $xy \in \mathbb{Q}^+$.

Proof: Left to the reader.

Theorem: The natural ordering of $\mathbb{Q}$ is dense, i.e. given $x, y \in \mathbb{Q}$ with $x < y$, there is a $z \in \mathbb{Q}$ such that $x < z$ and $z < y$.

Proof: Let $x,y \in \mathbb{Q}$ with $x < y$. Take $z = (x+y)/z$. Then $z - x = (y-x)/z \in \mathbb{Q}^+$.
Also $y-z = (y-x)/z \in \mathbb{Q}^+$. We have, therefore, $x < z$ and $z < y$.

■

Real Numbers

- We only need to use the properties of an integral domain in order to construct the reals from the rationals. We will denote the set of rationals by **R**.

Proposition: There is no rational number whose square is 2.

Proof: Let m.n be a rational number such that $(m/n)^2 = 2$.
Take ma nd n to be relatively prime integers (they have no common factors exceeding one.)
$(m/n)^2 = 2$ $\quad m^2/n^2 = 2$ $\quad m^2 = 2n^2$, hence m^2 is even, and thus m is even. Write $m = 2p$ for some integer p.
Thus $(2p)^2 = 2n^2$ $\quad 4p^2 = 2n^2$ $\quad 2p^2 = n^2$

hence, n^2 is even and thus n is even and can be written as n = 2q for some integer q. Thus, m and n have a common factor of 2, contrary to the assumption that m and n are relatively prime. Thus there is no rational number whose square is 2.

■

Construction of the Real Numbers –

Definition: A <u>Dedekind Cut</u> is a subset α of **R** such that

a) $\alpha \neq \emptyset$ and $\alpha^c \neq \emptyset$ (where $\alpha^c \neq \mathbf{R} - \alpha$)
b) $r \in \alpha$, $s \in \mathbf{R}$ and $r < s$ imply $s \in \alpha$ and
c) α does not have a minimum.

- Let *R* denote the set of all cuts.

Definition: A <u>rational cut</u> based on r_0 is the set $\{r : r \in R \text{ and } r > r_0\}$.

Definition: An <u>irrational cut</u> is any member of *R* that is not of this form.

- A cut is rational if and only if its compliment has a maximum.
- Special instances of the rational cuts are the zero cut θ and the unit cut δ
  - $\theta = \{ r : r \in \mathbf{R} \text{ and } r > 0\}$
  - $\delta = \{ r : r \in \mathbf{R} \text{ and } r > 1\}$

Example: $\gamma = \{ r : r \in R, r \geq 0 , \text{ and } r^2 > 2\}$ is a cut.

a) γ is non-empty since $s \in \gamma$, γ^c is non-empty since 1 is not in γ
b) Does $r < s$ imply $s \in \gamma$? Since $r^2 > 2$, $s > r$ implies $s^2 > 2$, so $s \in \gamma$.
c) Show that γ has not minimum
Let $s = (2r + 2)/(r+2)$. Since $r \geq 0$, $s \geq 0$;
$s^2 – 2 = (2r + 2 / r + 2)^2 = (sr + 2)^2/(r+2)^2 – 2 = 2(r^2 – 2)/(r+2)^2$.
Since $r^2 > 2$; $s^2 – 2 > 0$, so $s^2 > 0$.
Thus $s \in \gamma$, but
$s – r = (2r + 2)/(r+2) – r(r+2)/(r+2) = (2 - r^2)/(r + 2) < 0$.
Thus $s < r$ and γ does not have a minimum, and thus γ is a cut.
d) Show that γ is irrational
To show that γ is an irrational cut we must establish that γ^c does not have a maximum.

■

- For any cut α, $s \in \alpha^c$ and $r < s$ imply that $r \in \alpha^c$.
- If $s \in \alpha^c$ and $t \in \alpha$, then $s < t$. Although t must exceed s, it is possible to chose s and t as near as is desired.

Order –

- Order in *R* is defined in terms of set inclusion. Thus for cuts α and β we write $\alpha \leq \beta$ if and only if $\beta \subset \alpha$.

Proposition: $\leq$ is a linear order.

Proof: $\alpha \leq \alpha$ since $\alpha \subset \alpha$.

Since $\beta \subset \alpha$, and $\gamma \subset \beta$ $\gamma \subset \alpha$, $\alpha \leq \beta$ and $\beta \leq \gamma \Rightarrow \alpha \leq \gamma$.

Since $\beta \subset \alpha$ and $\alpha \subset \beta$ imply that $\alpha = \beta$, $\alpha \leq \beta$ and $\beta \leq \alpha \Rightarrow \alpha = \beta$.

To establish linearity of the order, suppose that $\alpha \neq \beta$.

Without loss of generality, we can assume that there is an r such that $r \in \alpha$ and $r \notin \beta$, so $r \in \beta^c$. If $s \in \beta$, then $r < s$ so that $s \in \alpha$; $\beta \subset \alpha$, so $\alpha \leq \beta$.

■

- A nonempty subset of *R* that is bounded below has an infimum. (Proof omitted)

Addition –

Definition: The <u>sum</u> of members α and β of *R* is defined to be

$\alpha + \beta = \{ r + s : r \in \alpha \text{ and } s \in \beta\}$.

- The sum of two cuts is the set of all sums of rational numbers that can be formed by adding a member of α to a member of β.

Proposition - $\alpha + \beta$ is a cut.

Proof:

a) Show $\alpha + \beta$ and $(\alpha + \beta)^c$ are non-empty

a. $\alpha + \beta$ is non-empty since both α and β are non-empty

b. Let $r_1 \in \alpha^c$ and $s^1 \in \beta^c$. Assume that $r_1 + s_1 \in \alpha + \beta$, and derive a contradiction. For some $r_2 \in \alpha$ and some $s_2 \in \beta$, $r + s_1 = r_2 + s_2$, but $r_1 < r_2$ and $s_1 < s_2$ by definition. This is impossible, thus $(\alpha + \beta)^c$ is non-empty.

b) Show $u \in \alpha + \beta$ and $u < t \Rightarrow t \in \alpha + \beta$. Let $r \in \alpha$, $s \in \beta$ and $r + s < t$. $t = r + (t - r)$, so $s < t - r$, thus $t - r \in \beta$, and $t \in \alpha + \beta$, $u \in \alpha + \beta$ and $u < t \Rightarrow t \in \alpha + \beta$.

c) Show $\alpha + \beta$ has no minimum. Let $r + s \in \alpha + \beta$ with $r \in \alpha$ and $s \in \beta$, so there exists a $t \in \alpha$ with $t < r$. (Since α has no minimum.)
Thus $t + 2 \in \alpha + \beta$ and $t + s < r + s$, so $\alpha + \beta$ has no minimum.

From a, b, and c we see that $\alpha + \beta$ is a cut.

- The sum of rational cuts based on a and b respectively, is the rational cut based on a + b.
- $\alpha + \beta = \beta + \alpha$
- $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
- The previous two rules are consequences of the definition of sum and properties of rational numbers.

Theorem: $\alpha + \theta = \alpha$

Proof: Let $r \in \alpha + \theta$, so $r = s + t$ for $s \in \alpha$ and $t \in \theta$.
Thus $s < s + t$, so $s + t \in \alpha$.
Thus $\alpha + \theta \subset \alpha$.
Let $r \in \alpha$, there is some $s \in \alpha$ such that $s \leq r$.
Thus $r = s + (r - s)$ and $r - s > 0$, $r \in \alpha + \theta$. So $\alpha \subset \alpha + \theta$.
Thus $\alpha = \alpha + \theta$.

■

Definition: The <u>negative</u> $-\alpha$ of a cut α is defined to be the set of all rational numbers r such that $-r$ is in α^c is not the maximum of that set (if such a maximum exists. In symbols:

$$-\alpha = \{ r : -r \in \alpha^c \text{ and } -r \neq \max \alpha^c \}$$

Proposition: $-\alpha$ is a cut.

Proof: Omitted.

Theorem: $\alpha + (-\alpha) = \theta$.

Proof: Let $r \in \alpha$ and $s \in -\alpha$, then
$-s \in \alpha^c$, $-s < r$, $o < r + s$, $r + s \in \theta$, so $\alpha + (-\alpha) \subset \theta$.
Let r be a member of θ so that $r > 0$. $\exists\, t_1, t_2 \in R$ such that $t_1 \in \alpha^c$, $t_2 \in \alpha$ and $0 < t_1 - t_2 < r$. W.L.O.G. assume t_1 is not the largest member of α^c.
$-t_1 \in -\alpha$ so $t_2 - t_1 \in \alpha + (-\alpha)$.
$t_2 - t_1 < r \Rightarrow r \in \alpha + (-\alpha)$, hence $\theta \subset \alpha + (-\alpha)$

■

Theorem: $\alpha \leq \beta$ implies $\alpha + \gamma \leq \beta + \gamma$

Proof: $\alpha \leq \beta \Rightarrow \beta \subset \alpha$
$\gamma + \gamma \subset \alpha + \gamma \Rightarrow \alpha + \gamma \leq \beta + \gamma$.

■

- So far, we have shown that *R* has an additive identity, additive inverse, is associative and commutative under addition, and is linearly ordered.

Multiplication –

Definition: Let *R'* – $\{ \alpha : \alpha \geq \theta \}$. The <u>product</u> $\alpha\beta$ of members α and α of *R'* is defined to be the set

$$\alpha\beta = \{ r : r \in \alpha \text{ and } s \in \beta \}$$

- $\alpha\beta$ is a cut (Proof similar to that of $\alpha + \beta$).

- Multiplication in *R'* is commutative and associative. i.e. $\alpha\beta = \beta\alpha$ for $\alpha, \beta \in R'$. $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ for $\alpha, \beta, \gamma \in R'$.

Theorem: δ (the unit cut) is the multiplicative identity, i.e. $\alpha\delta = \alpha$ for $\alpha \in$ *R'*.

Proof: Let $r \in \alpha$ and $s \in \delta$, then $r < rs$, $rs \in \alpha$, $\alpha\delta \subset \alpha$.
Let $r \in \alpha$, then $\exists\, u \in \alpha$ such that $u < r$.
Since α is non-negative, u is positive, u^{-1} exists.
$1 < ru^{-1}$ so $ru^{-1} \in \delta$. $r = u(ru^{-1})$, $r \in \alpha\delta$.
Thus, $\alpha \subset \alpha\delta$.

■

Multiplication interacts properly with addition and order –

- $\alpha (\beta + \gamma) = \alpha\beta + \alpha\gamma$ for $\alpha, \beta, \gamma \in$ *R'*.

Proposition: $\alpha \leq \alpha \Rightarrow \alpha\gamma \leq \beta\gamma$ for $\alpha, \beta, \gamma \in$ *R'*.

Proof: If $\alpha \leq \beta$, then $\beta \subset \alpha$ so that $\beta\gamma \subset \alpha\gamma$, hence, $\alpha\gamma \leq \beta\gamma$.

Definition: The <u>inverse</u> α^{-1} of a positive cut α is defined to be the set
$\alpha^{-1} = \{ r : r > 0, r^{-1} \in \alpha^c, \text{ and } r^{-1} \neq \max \alpha^c\}$

- α^{-1} is a positive cut

Theorem: $\alpha\alpha^{-1} = \delta$ for any $\alpha > \theta$.

Proof: Omitted.

- This construction of multiplication on the set of non-negative cuts can be extended to all of *R*.
- *R* is a complete ordered field.
- The set of rational cuts is the rational subfield of *R* and is isomorphic to the set of rational numbers. The irrational cuts are the irrational numbers.