Kris Harper
MATH 16100
Miklós Abért
October 23, 2007

Homework 4

Theorem 1 *$\sim$ is an equivalence relation on P.*

Proof. Let $(a,b) \in P$. Then $ab = ab$ and so $(a,b) \sim (a,b)$. Hence, reflexivity applies to $\sim$. Now let $(a_1,b_1),(a_2,b_2) \in P$ such that $(a_1,b_1) \sim (a_2,b_2)$. Then $a_1b_2 = a_2b_1$ and so $a_2b_1 = a_1b_2$. Thus $(a_2,b_2) \sim (a_1,b_1)$ and so symmetry holds for $\sim$. Now suppose $(a_1,b_1),(a_2,b_2),(a_3,b_3) \in P$ such that $(a_1,b_1) \sim (a_2,b_2)$ and $(a_2,b_2) \sim (a_3,b_3)$. Then $a_1b_2 = a_2b_1$ and $a_2b_3 = a_3b_2$. Multiplying the first equation by b_3 we have $a_1b_2b_3 = a_2b_1b_3$. But then since $a_2b_3 = a_3b_2$ we have $a_1b_2b_3 = a_3b_1b_2$ and dividing by $b_2 \neq 0$ we have $a_1b_3 = a_3b_1$. Therefore $(a_1,b_1) \sim (a_3,b_3)$ implying transitivity and since all three conditions have been met, $\sim$ is an equivalence relation on P. $\square$

Theorem 2 *If $(a_1,b_1) \sim (c_1,d_1)$ and $(a_2,b_2) \sim (c_2,d_2)$ then*

$$(a_1b_2 + a_2b_1, b_1b_2) \sim (c_1d_2 + c_2d_1, d_1d_2)$$

and

$$(a_1a_2, b_1b_2) \sim (c_1c_2, d_1d_2)$$

.

Proof. Let $(a_1,b_1) \sim (c_1,d_1)$ and $(a_2,b_2) \sim (c_2,d_2)$. Then we have $a_1d_1 = b_1c_1$ and $a_2d_2 = b_2c_2$. We multiply the first equation by b_2d_2 so we have $a_1b_2d_1d_2 = b_1b_2c_1d_2$ and we multiply the second equation by b_1d_1 so we have $a_2b_1d_1d_2 = b_1b_2c_2d_1$. Now we add the two new equations together so we have $a_1b_2d_1d_2 + a_2b_1d_1d_2 = b_1b_2c_1d_2 + b_1b_2c_2d_1$ and so $(a_1b_2 + a_2b_1)d_1d_2 = (c_1d_2 + c_2d_1)b_1b_2$ which implies $(a_1b_2 + a_2b_1, b_1b_2) \sim (c_1d_2 + c_2d_1, d_1d_2)$. Similarly, if we multiply $a_1d_1 = b_1c_1$ and $a_2d_2 = b_2c_2$ together we have $a_1a_2d_1d_2 = b_1b_2c_1c_2$ and so $(a_1a_2, b_1b_2) \sim (c_1c_2, d_1d_2)$. $\square$

Theorem 3 (Associativity of Addition) *For all $p,q,r \in \mathbb{Q}$ we have $(p+q)+r = p+(q+r)$.*

Proof. Let $p,q,r \in \mathbb{Q}$ such that $(p_1,p_2) \in p$, $(q_1,q_2) \in q$ and $(r_1,r_2) \in r$. Then we see that

$$\begin{aligned}
(p+q)+r &= \left(\overline{(p_1,p_2)} + \overline{(q_1,q_2)}\right) + \overline{(r_1,r_2)} \\
&= \overline{(p_1q_2 + p_2q_1, p_2q_2)} + \overline{(r_1,r_2)} \\
&= \overline{((p_1q_2 + p_2q_1)r_2 + p_2q_2r_1, p_2q_2r_2)} \\
&= \overline{(p_1q_2r_2 + p_2q_1r_2 + p_2q_2r_1, p_2q_2r_2)} \\
&= \overline{((q_1r_2 + q_2r_1)p_2 + p_1q_2r_2, p_2q_2r_2)} \\
&= p + \overline{(q_1r_2 + q_2r_1, q_2r_2)} \\
&= p + (q+r).
\end{aligned}$$

$\square$

Theorem 4 (Additive Identity) *There exists an $n \in \mathbb{Q}$ such that for all $p \in \mathbb{Q}$ we have $n + p = p$. Show that n is unique.*

Proof. We see that if we let $n \in \mathbb{Q}$ such that $n = \overline{(0,1)}$ and if we let $(p_1, p_2) \in p$ for some $p \in \mathbb{Q}$ then we have $n + p = \overline{(0,1)} + \overline{(p_1,p_2)} = \overline{((0)p_2 + (1)p_1, (1)p_2)} = \overline{(p_1,p_2)} = p$. Now suppose there exist two additive identities such that for all $p \in \mathbb{Q}$ we have $n_1 + p = p$ and $n_2 + p = p$. Then we have $n_2 = n_1 + n_2 = n_2 + n_1 = n_1$ and so $n_1 = n_2$. Thus, the additive identity is unique. (This uses Theorem 6 which is proved without use of the additive identity.) □

Theorem 5 (Additive Inverse) *For all $p \in \mathbb{Q}$ there exists $q \in \mathbb{Q}$ such that $p + q = 0$. Show that q is unique.*

Proof. Let $p \in \mathbb{Q}$ such that $(p_1, p_2) \in p$. Then we choose $q = \overline{(-p_1, p_2)}$ for $q \in \mathbb{Q}$. Then we have $p + q = \overline{(p_1,p_2)} + \overline{(-p_1,p_2)} = \overline{(p_1p_2 + -p_1p_2, p_2p_2)} = \overline{(0, p_2p_2)} = \overline{(0,1)} = 0$ since $(0)p_2p_2 = (0)(1)$. Now suppose there exist two additive inverses so that $p + n_1 = 0$ and $p + n_2 = 0$. Then we have $p + n_1 = p + n_2$ and adding $\overline{(-p_1,p_2)}$ to both sides we have $\overline{(-p_1,p_2)} + \overline{(p_1,p_2)} + n_1 = \overline{(-p_1p_2 + p_1p_2, p_2p_2)} + n_1 = 0 + n_1$ on the left and $\overline{(-p_1,p_2)} + \overline{(p_1,p_2)} + n_2 = \overline{(-p_1p_2 + p_1p_2, p_2p_2)} + n_2 = 0 + n_2 = n_2$ on the right. So $n_1 = n_2$. (Again, this uses Theorem 4, which uses Theorem 6, which is proved without Theorems 4 or 5.) □

Theorem 6 (Commutativity of Addition) *For all $p, q \in \mathbb{Q}$ we have $p + q = q + p$.*

Proof. Let $p, q \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and $(q_1, q_2) \in q$. Then we have $p + q = \overline{(p_1,p_2)} + \overline{(q_1,q_2)} = \overline{(p_1q_2 + p_2q_1, p_2q_2)} = \overline{(q_1p_2 + q_2p_1, q_2p_2)} = \overline{(q_1,q_2)} + \overline{(p_1,p_2)} = q + p$. □

Theorem 7 (Associativity of Multiplication) *For all $p, q, r \in \mathbb{Q}$ we have $(p \cdot q) \cdot r = p \cdot (q \cdot r)$.*

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p$, $(q_1, q_2) \in q$ and $(r_1, r_2) \in r$. Then we have $(p \cdot q) \cdot r = \left(\overline{(p_1,p_2)} \cdot \overline{(q_1,q_2)}\right) \cdot \overline{(r_1,r_2)} = \overline{(p_1q_1, p_2q_2)} \cdot \overline{(r_1,r_2)} = \overline{(p_1q_1r_1, p_2q_2r_2)} = p \cdot \overline{(q_1r_1, q_2r_2)} = p \cdot (q \cdot r)$. □

Theorem 8 (Multiplicative Identity) *There exists $e \in \mathbb{Q}$ such that for all $p \in \mathbb{Q}$ we have $e \cdot p = p$.*

Proof. Let $p \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and let $e \in \mathbb{Q}$ such that $e = \overline{(1,1)}$. Then we have $e \cdot p = \overline{(1,1)} \cdot \overline{(p_1,p_2)} = \overline{(p_1(1), p_2(1))} = p$. Suppose there exist two multiplicative identities e_1 and e_2 such that for all $p \in \mathbb{Q}$ $e_1 \cdot p = p$ and $e_2 \cdot p = p$. Then we have $e_1 = e_2 \cdot e_1$ and $e_2 = e_1 \cdot e_2 = e_2 \cdot e_1$. So we have $e_1 = e_2$. (This uses Theorem 10 which is proved without use of the multiplicative identity.) □

Theorem 9 (Multiplicative Inverse) *For all $p \in \mathbb{Q}$ with $p \neq 0$ there exists $q \in \mathbb{Q}$ such that $p \cdot q = 1$.*

Proof. Let $p \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and since $p_1 \neq 0$ let $q \in \mathbb{Q}$ such that $(p_2, p_1) \in q$. Then we see that $p \cdot q = \overline{(p_1,p_2)} \cdot \overline{(p_2,p_1)} = \overline{(p_1p_2, p_1p_2)} = \overline{(1,1)} = 1$. Now suppose there are two multiplicative inverses for some $p \in \mathbb{Q}$ such that $p \cdot q_1 = 1$ and $p \cdot q_2 = 1$. Then, multiplying both equations by $\overline{(p_2,p_1)}$, we have $q_1 = \overline{(1,1)} \cdot q_1 = \overline{(p_1p_2, p_1p_2)} \cdot q_1 = \overline{(p_2,p_1)} \cdot \overline{(p_1,p_2)} \cdot q_1 = \overline{(p_2,p_1)} \cdot \overline{(p_1,p_2)} \cdot q_2 = \overline{(p_1p_2, p_1p_2)} \cdot q_2 = \overline{(1,1)} \cdot q_2 = q_2$. (Once again, this uses Theorem 8, which uses Theorem 10, which is proved without use of Theorems 8 or 9.) □

Theorem 10 (Commutativity of Multiplication) *For all $p, q \in \mathbb{Q}$ we have $p \cdot q = q \cdot p$.*

Proof. Let $p, q \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and $(q_1, q_2) \in q$. Then $p \cdot q = \overline{(p_1,p_2)} \cdot \overline{(q_1,q_2)} = \overline{(p_1q_1, p_2q_2)} = \overline{(q_1p_1, q_2p_2)} = \overline{(q_1,q_2)} \cdot \overline{(p_1,p_2)} = q \cdot p$. □

Theorem 11 (Distributivity) *For all $p, q, r \in \mathbb{Q}$ we have $p \cdot (q + r) = p \cdot q + p \cdot r$.*

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p$, $(q_1, q_2) \in q$ and $(r_1, r_2) \in r$. Then we have

$$\begin{aligned} p \cdot (q + r) &= \overline{(p_1, p_2)} \cdot \left(\overline{(q_1, q_2)} + \overline{(r_1, r_2)}\right) \\ &= \overline{(p_1, p_2)} \cdot \overline{(q_1 r_2 + q_2 r_1, q_2 r_2)} \\ &= \overline{(p_1 q_1 r_2 + p_1 q_2 r_1, p_2 q_2 r_2)} \\ &= \overline{(p_1 q_1 r_2 + p_1 q_2 r_1, p_2 q_2 r_2)} \cdot \overline{(p_2, p_2)} \\ &= \overline{(p_1 p_2 q_1 r_2 + p_1 p_2 q_2 r_1, p_2 p_2 q_2 r_2)} \\ &= \overline{(p_1 q_1, p_2 q_2)} + \overline{(p_1 r_1, p_2 r_2)} \\ &= \overline{(p_1, p_2)} \cdot \overline{(q_1, q_2)} + \overline{(p_1, p_2)} \cdot \overline{(r_1, r_2)} \\ &= p \cdot q + p \cdot r. \end{aligned}$$

□

Theorem 12 *The function $f : \mathbb{Z} \to \mathbb{Q}$ where $f(n) = \overline{(n, 1)}$ is injective.*

Proof. Let $a, b \in \mathbb{Z}$ such that $f(a) = f(b)$. Then we have $\overline{(a, 1)} = \overline{(b, 1)}$ and so $(a, 1) \sim (b, 1)$ which implies $a = b$. □

Theorem 13 *For all $m, n \in \mathbb{Z}$ we have*

$$f(m + n) = f(m) + f(n) \text{ and } f(mn) = f(m) \cdot f(n).$$

Proof. Let $m, n \in \mathbb{Z}$. Then we have
$f(m + n) = \overline{(m + n, 1)} = \overline{(m(1) + n(1), (1)(1))} = \overline{(m, 1)} + \overline{(n, 1)} = f(m) + f(n)$. Additionally we see that $f(mn) = \overline{(mn, (1)(1))} = \overline{(m, 1)} \cdot \overline{(n, 1)} = f(m) \cdot f(n)$. □

Theorem 14 *For every rational number $r \in \mathbb{Q}$ there exist $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $r = mn^{-1}$.*

Proof. Let $r \in \mathbb{Q}$ such that $(m, n) \in r$ (since r is nonempty). Then we see $m, n \in \mathbb{Z}$. Thus we can write $m = \overline{(m, 1)}$ and $n = \overline{(n, 1)}$. And so $n^{-1} = \overline{(1, n)}$ since $n \neq 0$ and we have
$m \cdot n^{-1} = \overline{(m, 1)} \cdot \overline{(1, n)} = \overline{(m, n)} = r$. □

Lemma 15 *Any element in $\mathbb{Q}$ can be written as $\overline{(a, b)}$ with $b > 0$.*

Proof. Let $\overline{(a, b)} \in \mathbb{Q}$. There are two cases:

Case 1: If $b > 0$ then we are done.

Case 2: If $b < 0$ then we have $a(-b) = -ab = (-a)b$ and so $(a, b) \sim (-a, -b)$. Thus $\overline{(a, b)} = \overline{(-a, -b)}$ and $-b > 0$. □

Theorem 16 *Show that $<$ is a well-defined relation on $\mathbb{Q}$.*

Proof. Let $\overline{(a_1, b_1)}, \overline{(a_2, b_2)}, \overline{(c_1, d_1)}, \overline{(c_2, d_2)} \in \mathbb{Q}$ such that $\overline{(a_1, b_1)} < \overline{(a_2, b_2)}$ and $(a_1, b_1) \sim (c_1, d_1)$ and $(a_2, b_2) \sim (c_2, d_2)$. We take b_1, b_2, d_1 and d_2 to all be greater than 0 by Lemma 15. Then we have $a_1 b_2 < a_2 b_1$ and so $a_1 b_2 d_1 d_2 < a_2 b_1 d_1 d_2$. But we also know that $a_1 d_1 = b_1 c_1$ and $a_2 d_2 = b_2 c_2$. Making the appropriate substitutions we see $b_1 b_2 c_1 d_2 < b_1 b_2 c_2 d_1$. Since $b_1 b_2 > 0$ we have $c_1 d_2 < c_2 d_1$ and so $\overline{(c_1, c_2)} < \overline{(d_1, d_2)}$. This shows that $<$ is well-defined. □

Theorem 17 *The relation $<$ is an ordering on $\mathbb{Q}$.*

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p$, $(q_1, q_2) \in q$ and $(r_1, r_2) \in r$. By Lemma 15 we let p_2, q_2 and r_2 all be greater than 0. If $p \neq q$ then we see that $(p_1, p_2) \nsim (q_1, q_2)$ and so $p_1q_2 \neq p_2q_1$. Then we have have either $p_1q_2 < p_2q_1$ and so $p < q$ or $p_2q_1 < p_1q_2$ and so $q < p$. Secondly if $p < q$ then we have $p_1q_2 < p_2q_1$ and so $p_1q_2 \neq p_2q_1$. Therefore $(p_1, p_2) \nsim (q_1, q_2)$. Thus $p \neq q$. Finally, if $p < q$ and $q < r$ then $p_1q_2 < p_2q_1$ and $q_1r_2 < q_2r_1$. Multiplying the first inequality by r_2 and the second by p_2 we have $p_1q_2r_2 < p_2q_1r_2$ and $p_2q_1r_2 < p_2q_2r_1$ since $p_2 > 0$ and $r_2 > 0$. This implies $p_1q_2r_2 < p_2q_2r_1$ and since $q_2 > 0$ we have $p_1r_2 < p_2r_1$ and so $p < r$. Since all three conditions are satisfied, we see that $<$ is an ordering on $\mathbb{Q}$. $\square$

Exercise 18 *Is $(\mathbb{Q}, <)$ a model of C? That is, which axioms does it satisfy.*

Proof. Since the integers are a subset of $\mathbb{Q}$ and there exists at least one integer and since we showed that $<$ was and ordering on $\mathbb{Q}$, we see that axioms 1 and 2 are satisfied. Theorem 20 shows that there is no last point of $\mathbb{Q}$. To show that there is no first point we use a similar argument. Let $\overline{(a, b)} \in \mathbb{Q}$ such that $b > 0$. We again consider three cases:

Case 1: Let $a > 0$. Then $a(1) > (0)b$ and so $\overline{(a, b)} > \overline{(0, 1)} = 0$.

Case 2: Let $a < 0$. Then since $b > 0$, $a > ab - b$ which means $\overline{(a, b)} > \overline{(a - 1, 1)} = a - 1$.

Case 3: Let $a = 0$ then $\overline{(a, b)} = \overline{(0, b)} = 0$ and since $-1 < 0$ we see $\overline{(a, b)} > \overline{(-1, 1)} = -1$.

So we see that for any element of $\mathbb{Q}$ there is always an element greater than it and an element less than it which means it can have no first or last point and so it satisfies axiom 3. $\square$

Theorem 19 *For every $p, q \in \mathbb{Q}$ such that $p < q$ there exists $r \in \mathbb{Q}$ such that $p < r < q$.*

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p$, $(q_1, q_2) \in q$ and $r = \overline{(p_1q_2 + p_2q_1, 2p_2q_2)}$. Let $p < q$ and by Lemma 15 let $p_2 > 0$ and $q_2 > 0$. Then we have $p_1q_2 < p_2q_1$ and so $p_1p_2q_2 < p_2p_2q_1$ which implies $2p_1p_2q_2 < p_1p_2q_2 + p_2p_2q_1$. We see that this implies $\overline{(p_1, p_2)} < \overline{(p_1q_2 + p_2q_1, 2p_2q_2)}$ which means $p < r$. Similarly, we have $p_1q_2 < p_2q_1$ which means $p_1q_2q_2 < p_2q_1q_2$ and $p_1q_2q_2 + p_2q_1q_2 < 2p_2q_1q_2$. This implies $\overline{(p_1q_2 + p_2q_1, 2p_2q_2)} < \overline{(q_1, q_2)}$ which means $r < q$. Thus $p < r < q$. $\square$

Theorem 20 *For every $p \in \mathbb{Q}$ there exists $n \in \mathbb{Z}$ such that $p < n$.*

Proof. Let $p \in \mathbb{Q}$ such that $(a, b) \in p$. Let $b > 0$ by Lemma 15. We have to consider three cases:

Case 1: Let $a > 0$. Then $a < ab + b$ and so $\overline{(a, b)} < \overline{(a + 1, 1)} = a + 1$.

Case 2: Let $a < 0$. Then $a(1) < b(0)$ and so $\overline{(a, b)} < \overline{(0, 1)} = 0$.

Case 3: Let $a = 0$. Then $\overline{(a, b)} = \overline{(0, b)} = \overline{(0, 1)} = 0$ and since $0 < 1$ we see $\overline{(a, b)} < \overline{(1, 1)} = 1$. $\square$