Math 650.2 Homework 8

Elliot Gangaram
elliot.gangaram@gmail.com

Problem 1

Show that the multiplication of cuts respects the multiplicative field axioms and the distributive axiom. (This is step 6 in Dedekind's construction).

We will first show that multiplication of **positive** cuts respects the multiplicative and distributive field axioms. Therefore, we shall restrict ourselves to $\mathbb{R}^+$, which refers to the set of all cuts, $\alpha \in \mathbb{R}$ such that $\alpha > 0^*$. In order to show multiplication respects the field axioms, we first must define how to multiply cuts. If $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$, then it is natural to define the set $\alpha\beta$ to be the set of all p such that $p \leq rs$ for some choice of $r \in \alpha$, and $s \in \beta$, such that $r > 0$ and $s > 0$. Let us also define the set which we will soon see turns out to be the multiplicative identity. The set we are talking about is 1^* which refers to the set of all $q < 1$ for $q \in \mathbb{Q}$. We shall now verify axiom $M1$, the closure property.

To show closure we must show that the product, $\alpha\beta$ is a cut by showing that $\alpha\beta$ fulfills the properties of cuts.

Property One: It is clear that $\alpha\beta$ is not empty. Since α and β by assumption are cuts which are defined to be nonempty, there is at least one element in α and at least one element in β. Let $r \in \alpha$ and $s \in \beta$. Then the element $rs \in \alpha\beta$.
Additionally, $\alpha\beta \neq \mathbb{Q}$. To see this, note by the definition of cuts, there exists a rational number $r' \notin \alpha$ and similarly, there exists a rational number $s' \notin \beta$. Then, from our definition of cuts, $r < r'$ and $s < s'$ which shows $rs < r's'$. Thus, $r's' \notin \alpha\beta$ and so $\alpha\beta \neq \mathbb{Q}$.

Property Two: We would like to show that if $p \in \alpha\beta$, $q \in \mathbb{Q}$ and $q < p$, then $q \in \alpha\beta$. By our definition of multiplication, if $p \in \alpha\beta$, then $p = rs$ where $r \in \alpha$ and $s \in \beta$. Since $q < p$ by assumption, we have $q < rs$ which implies $q/s < r$. Again by our definition of cuts, since $q/s < r$, then $q/s \in \alpha$. But since $q/s \in \alpha$, and $s \in \beta$, then $(q/s)s \in \alpha\beta$ which shows that $q \in \alpha\beta$.

Property Three: We must show if $p \in \alpha\beta$, then $p < z$ for some $z \in \alpha\beta$. As defined before, let $p \in \alpha\beta$ such that $p = rs$ where $r \in \alpha$ and $s \in \beta$. By property three of the cut α, we know there exists an element $t \in \alpha$ such that $t > r$. Let $z = ts$. Then we have

$p = rs < ts = z$ Note that $z \in \alpha\beta$ since $t \in \alpha$ and $s \in \beta$ and also $p < z$ so we have proved property three for $\alpha\beta$. Thus, $\alpha\beta$ is a cut and axiom $M1$ holds.

Recall that axiom $A2$ states that the addition of elements in the set are commutative. As usual, let $\alpha\beta$ denote the set of all elements rs with $r \in \alpha$ and $s \in \beta$. We would like to show that $\alpha\beta = \beta\alpha$. Then, by the same way we have defined the multiplication of sets, $\beta\alpha$ refers to the set of all elements sr. However, s and r are elements of $\mathbb{Q}$ and so these elements commute. This means we have $rs = sr$ for all elements s and r which shows that $\alpha\beta = \beta\alpha$.

We now show that axiom $A3$, which asserts the associativity of elements under the operation in the field, holds. To show that the multiplication of cuts is associative requires the same strategy as above. Namely, we want to show that $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ where $\alpha,\ \beta$, and γ are cuts. Let $r \in \alpha,\ s \in \gamma$, and $c \in \gamma$. Then the element $r(sc) \in \alpha(\beta\gamma)$. However, since $r,\ s$, and c are in $\mathbb{Q}$, then we have $r(sc) = (rs)c \in (\alpha\beta)\gamma$. This holds for all such $r,\ s$, and c since these elements are arbitrary which tells us $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

Axiom $A4$ requires us to show that there exists a multiplicative identity. I claim that the additive identity in the set is 1^* where $1^* = \{q \in \mathbb{Q} \mid q < 1\}$. First of all, how do we know that 1^* is a cut? Let us prove that the definition of 1^* fulfills our definition of cuts.

Property One: Clearly 1^* is not empty since $0 \in 1^*$. It is also easy to see that $1^* \neq \mathbb{Q}$ since 1^* does not contain the rational number 2.

Property Two: We would like to show that if $p \in 1^*$, $q \in \mathbb{Q}$ and $q < p$, then $q \in 1^*$. Since $p \in 1^*$, then $p < 1$ which shows that $q < p < 1$. Therefore $q < 1$ and so $q \in 1^*$.

Property Three: We must show that if $p \in 1^*$, then $p < z$ for some $z \in 1^*$. This is immediate from the previous homework where we showed that $\mathbb{Q}$ is dense in $\mathbb{Q}$ and thus 1^* has no maximal element.

Now that we know 1^* is a cut, our objective is to show $\alpha 1^* = \alpha$. To show that two sets are equal, we must show that each set is a subset of the other set. We will first show that $\alpha 1^* \subseteq \alpha$. Let $r \in \alpha$ and $s \in 1^*$. Then by the definition of 1^*, we have $rs < r$ because . This tells is that $rs \in \alpha$ which implies $\alpha 1^* \subseteq \alpha$.

We would now like to show the other inclusion is true, namely $\alpha \subseteq \alpha 1^*$. Let $p \in \alpha$. We know there exists an $r \in \alpha$ such that $r > p$ by the definition of cuts. Then, $p/r \in 1^*$. This tells us that, $p = r(p/r) \in \alpha 1^*$. So we have $\alpha \subseteq \alpha 1^*$. Since $\alpha 1^* \subseteq \alpha$ and $\alpha \subseteq \alpha 1^*$, we have that $\alpha = \alpha 1^*$.

To complete this step we must show that axiom $A5$ holds. That is, for every element $\alpha \in \mathbb{R}^+$, there exists an element $\beta \in \mathbb{R}^+$ such that $\alpha\beta = 1^*$. Let $z \notin \alpha$. Define β to be the following set: $\beta = \{b \mid b < 1/z\}$. Again we are faced with the following question - how do know that β is a cut? Clearly, β is nonempty since β contains the number 0. Additionally, $\beta \neq \mathbb{Q}$. To see this, suppose $z \notin \alpha$. Then $z > a$ for all $a \in \alpha$. In particular, if $a > 0$, then $1/a > 1/z$ for all $z \notin \alpha$. This tells us that $1/a \notin \beta$ and thus $\beta \neq \mathbb{Q}$. This proves the first requirement of being a cut.

For the second property of cuts, let $b \in \beta$ and assume that $b' < b$. We want to show that $b' \in \beta$. Note that $b \in \beta$ implies that $b < 1/z$ and thus $b' < b < 1/z$ so $b' \in \beta$.
Now we must show that there is no maximal element in β. This follows directly from the denseness of $\mathbb{Q}$ in $\mathbb{Q}$ because whenever $b < 1/z$, there exists a rational number b' such that $b < b' < 1/z$ and thus $b' \in \beta$. So we have verified that β is a cut. It remains to seen that β is the multiplicative inverse of α.

As usual, we will show set equality. Let $a \in \alpha$, $a > 0$, and $b \in \beta$ such that $b > 0$. Then for some $z \notin \alpha$, we have $b < 1/z < 1/a$ where $1/z < 1/a$ follows from the fact that $z > a$. Therefore, multiplying $b < 1/z < 1/a$ throughout by a yields $ab < a/z < 1$ and so $\alpha\beta \subseteq 1^*$.

Now we want to show that $1^* \subseteq \alpha\beta$. Let $c \in 1^*$ such that $0 < c < 1$. Pick any positive $a' \in \alpha$. Then there are rationals $a < z$ where $a \in \alpha$, $z \notin \alpha$, with $a > 0$ such that $z - a < (1-c)(a')$. Then $1 - (a/z) = (z-a)/a = \dfrac{(1-c)a'}{z} < 1 - c$. This tells us that $a/z > c$ and $c/a < 1/z$. But, $c/a < 1/z$ suggests that $c/a \in \beta$ and so $c = (a)(c/a) \in \alpha\beta$ and thus $1^* \subseteq \alpha\beta$. The two set inclusions tells us that $1^* = \alpha\beta$ which completes the proof.

Lastly, we prove the distributive property. We would like to show $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ where α, β, and γ are cuts in $\mathbb{R}^+$. Let $a \in \alpha$, $b \in \beta$, $c \in \gamma$. Since the elements are rationals, then we have $a(b + c) = ab + ac$ which holds for all $a \in \alpha$, $b \in \beta$, $c \in \gamma$ and so we have $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Thus, multiplication and addition respects all the field axioms.

Problem 2

In step 6, the multiplication of cuts was defined for only $\mathbb{R}^+$. Show that the multiplicative and distributive axioms hold for all of $\mathbb{R}$. (This is step 7 in Dedekind's construction).

We now extend multiplication to cuts that are less than 0^* by the following piece wise defined function.

$$\alpha\beta = \begin{cases} (\alpha)(\beta), & \text{if } \alpha > 0^*, \beta > 0^* \\ (-\alpha)(-\beta), & \text{if } \alpha < 0^*, \beta < 0^* \\ -[(-\alpha)(\beta)], & \text{if } \alpha < 0^*, \beta > 0^* \\ -[(\alpha)(-\beta)], & \text{if } \alpha > 0^*, \beta < 0^* \\ 0^*, & \text{if } \beta = 0^* \end{cases}$$

Note that the defined operations do indeed satisfy the axioms, although they are cumbersome to check since this requires doing roughly the same procedures in step 6 for the additional 3 cases.

Problem 3

Show if $a \in \cup_{i\in\mathcal{I}} A_i$ then $a \in A_j$ where $j \in \mathcal{I}$.

By Zermelo-Fraenkel set theory, the Axiom of Union states for any set S, there exists a set U such that $x \in U$ if and only if $x \in A$ for some $A \in S$. As an example, let $S = \{\{1,2\},\{3,4\}\}$. Then $U = \{1,2,3,4\}$. We would like to show that if $a \in \cup_{i\in\mathcal{I}} A_i$ then $a \in A_j$ where $j \in \mathcal{I}$. Consider $\cup_{i\in\mathcal{I}} A_i$. This is telling us there is a set U such that the elements belong to the set U if and only if the elements belong to some set A where A belongs to S. So let us take $\cup_{i\in\mathcal{I}} A_i$ to be the set U. By assumption $a \in \cup_{i\in\mathcal{I}} A_i$. By our axiom, this tells us that $a \in A_j$.

Problem 4

Given an explicit function, $f : \mathbb{Q} \to \mathbb{N}$ to show that $\mathbb{Q}$ is countable.

From the previous homework, we have shown that $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ defined by $f(p/q) = (p,q)$ where p and q are relatively prime is injective, and $g : \mathbb{Z} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined by $g(x,y) = (\phi^{-1}(x), y)$ is a bijection. We also showed that $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $h(m,n) = 2^{m-1}(2n-1)$ is a bijection. Thus, $h \circ g \circ f : \mathbb{Q} \to \mathbb{N}$ is a one to one function. This function proves that $\mathbb{Q}$ is countable. To see this, note that $h \circ g \circ f$ is a injection. Moreover, $h \circ g \circ f : \mathbb{Q} \to h(g(f(\mathbb{Q})))$ is a bijection since the codomain is exactly the range. However, $h(g(f(\mathbb{Q}))) \subset \mathbb{N}$ and by Theorem 2.8 in Rudin, or from Problem 4 in Homework 7, we can conclude that $\mathbb{Q}$ is countable. Note that $h(g(f(p,q))) = 2^{\phi^{-1}(p)-1}(2q-1)$.

Problem 5

Prove that $\mathbb{R}$ is uncountable.

Let us assume that $\mathbb{R}$ is countable. In that case, there exists a bijection $f : \mathbb{R} \to \mathbb{N}$. Moreover, if this is the case, then there exists a bijection $\phi : (0,1) \to \mathbb{N}$ since $(0,1)$ is a subset of $\mathbb{R}$ and we proved that a subset of a countable set is countable. So there exists a

bijection between the real numbers in the interval (0,1) to the set of natural numbers. If this is the case then these numbers can be written as decimals of the form:

$$\begin{gathered} 0.a_1a_2a_3 \ldots\ldots\ldots \rightarrow 1 \\ 0.b_1b_2b_3 \ldots\ldots\ldots \rightarrow 2 \\ 0.c_1c_2c_3 \ldots\ldots\ldots \rightarrow 3 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{gathered}$$

where the $a's$, $b's$, and $c's$ are digits which take on values in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Since there exists a bijection, let us list out a general one to one correspondence. Then the natural number 1 is associated to some decimal, call it $0.a_1a_2a_3 \ldots\ldots\ldots$, similarly the natural number 2 is associated to some decimal call it $0.b_1b_2b_3 \ldots\ldots\ldots$, the natural number 3 is associated to some decimal $0.c_1c_2c_3 \ldots\ldots\ldots$ and so on and so fourth. Since this is a general correspondence, if we can show that there exists some number in the interval $(0, 1)$ which is missed by the general correspondence, then it shows that the set is not countable. Let us attempt to construct such a number that is not in the set. Call this number $x = 0.x_1x_2x_3 \ldots$. Since we are constructing such a number, we are free to place the restrictions on this number. Let us place the following restrictions:

$$\begin{gathered} x_1 \neq a_1, 0, \text{ or } 9 \\ x_2 \neq b_2, 0, \text{ or } 9 \\ x_3 \neq c_3, 0, \text{ or } 9 \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{gathered}$$

The reason for doing so is that because we are attempting to reach a contradiction. That is, we want to find an x that is not equal to one of the numbers written in the decimal form above. Thus we have chosen for $x \neq .0000\ldots = 0$ and $x \neq .9999\ldots = 1$. Now by our construction of x, we see that $x \neq 0.a_1a_2a_3 \ldots\ldots$ since $x_1 \neq a_1$. Similarly $x \neq 0.b_1b_2b_3 \ldots\ldots$ because $x_2 \neq b_2$. Repeating this process indefinitely shows us that x does not equal to any number in the one to one correspondence. Thus, this contradicts the one to one correspondence and so we may conclude that the set of real numbers in $(0, 1)$, and therefore the set of real numbers, is uncountable.

Problem 6

Prove Theorem 2.8 in Rudin.

Theorem 2.8: Every infinite subset of a countable set A is countable.

Proof: Let $E \subset A$ and assume that E is infinite. Since A is countable, there exists a bijection $f : \mathbb{N} \rightarrow A$. We will denote the mapping of this function as $f(n) = x$. It is clear that $n \in \mathbb{N}$ and $x \in A$. Moreover, from Rudin's definition on page 26, we know that we can arrange the elements of A in a sequence. That is, we can list out the elements of A as

$x_1, x_2, x_3, \ldots$. where x_i denotes the $i \in \mathbb{N}$.

For example, $f(5) = x_5$. Note however, that Rudin uses J to denote the domain, or simply the set to which n belongs to. The reason for doing so is that the domain is either the set of nonnegative integers or $\mathbb{N}$. For concreteness, we are using the set of $\mathbb{N}$. In doing so, it makes the notation more intuitive. We now continue the proof.

So we can construct a sequence $x_1, x_2, x_3, \ldots$. Note that each $x_i \in A$ is not necessarily in E. As such let us construct a sequence of terms that belong to E. To do so, we proceed as follows: let n_1 be the smallest positive integer such that $x_{n_1} \in E$. This is saying, let n_1 be the smallest natural number such that $f(n_1)$ is some element in E. Now find a sequence of such natural numbers, denoted by $n_2, n_3, \ldots n_{k-1}, n_k$ for $k = 2, 3, 4, \ldots$ such that n_k is the smallest positive integer greater than n_{k-1} where each n_i, $1 \leq i \leq k$ has the property that $f(n_i) \in E$. Note that we are relying on the fact that the set of natural numbers is well ordered. In laymen's terms, what is happening is that our domain is the set of natural numbers and these natural numbers are mapping to something in A. We can order the set of natural numbers from least to greatest. Then, we go along this ordered list of natural numbers and choose the natural numbers which maps to an element in E. Now, we can set $f(k) = x_{n_k}$. In doing so, we are "matching" the elements in the domain to the elements in E. This matching is a 1 to 1 correspondence since every element in E comes from some element in $\mathbb{N}$ so the function is surjective. Moreover, it is clear this function is injective since if $f(a) = f(b)$, then we have $x_{n_a} = x_{n_b}$ so $a = b$. Thus we have created a one to one correspondence between $\mathbb{N}$ and the set E so it follows that E is countable.

Problem 7

Suppose $k \geq 3$, $\mathbf{x}$, $\mathbf{y} \in \mathbb{R}^k$, $|\mathbf{x} - \mathbf{y}| = d > 0$, and $r > 0$. Prove:

(a) If $2r > d$, there are infinitely many $\mathbf{z} \in \mathbb{R}^k$ such that $|\mathbf{z} - \mathbf{x}| = |\mathbf{z} - \mathbf{y}| = r$.

Let $\mathbf{w}$ be a vector satisfying the following two equations:

$$\mathbf{w} \cdot (\mathbf{x} - \mathbf{y}) = 0 \tag{1}$$

$$|\mathbf{w}|^2 = r^2 - \frac{d^2}{4} \tag{2}$$

From linear algebra, if $\mathbf{w}$ is any non-zero solution of the first equation, then there is a unique positive number t such that $t\mathbf{w}$ satisfies both equations. Since at least two components can vary independently, we can find a solution with these components having any desired ratio. This ratio does not change when we multiply by a positive number t. Since there are infinitely many ratios, it follows that there are infinitely many solutions. More specifically, for each solution $\mathbf{w}$, the vector $z = \frac{1}{2}\mathbf{x} + \frac{1}{2}\mathbf{y} + \mathbf{w}$ is

a solution of the required equation. To see this,

$$\begin{aligned} |\mathbf{z}-\mathbf{x}|^2 &= \left|\frac{\mathbf{y}-\mathbf{x}}{2}+\mathbf{w}\right|^2 \\ &= \left|\frac{\mathbf{y}-\mathbf{x}}{2}\right|^2 + 2\mathbf{w}\cdot\left(\frac{\mathbf{x}-\mathbf{y}}{2}\right) + |\mathbf{w}|^2 \\ &= \frac{d^2}{4} + 0 + r^2 - \frac{d^2}{4} \\ &= r^2 \end{aligned}$$

and a similar relation for $|\mathbf{z}-\mathbf{y}|^2$.

(b) If $2r = d$, there is exactly one such $\mathbf{z}$.

Since $2r = d$, we have $|\mathbf{x}-\mathbf{y}| = d = |\mathbf{x}-\mathbf{z}| + |\mathbf{z}-\mathbf{y}|$. So there exists a nonnegative scalar t such that $\mathbf{x}-\mathbf{z} = t(\mathbf{z}-\mathbf{y})$. By hypothesis, it follows that $t = 1$ and so $\mathbf{z}$ is uniquely determined as $\mathbf{z} = \dfrac{\mathbf{x}+\mathbf{y}}{2}$.

(c) If $2r < d$, there is no such $\mathbf{z}$.

If $d > 2r$, then substituting in $d = |\mathbf{x}-\mathbf{y}|$ and then we have $|\mathbf{x}-\mathbf{y}| > |\mathbf{x}-\mathbf{z}| + |\mathbf{z}-\mathbf{y}|$ which is the same as $|(\mathbf{x}-\mathbf{z}) + (\mathbf{z}-\mathbf{y})| > |\mathbf{x}-\mathbf{z}| + |\mathbf{z}-\mathbf{y}|$. This tells us that $|\mathbf{x}-\mathbf{y}| > |\mathbf{x}-\mathbf{z}| + |\mathbf{z}-\mathbf{y}|$ which violates the triangle inequality.