Math 650.2 Homework 7

Elliot Gangaram
elliot.gangaram@gmail.com

Problem 1

Verify that the axioms for addition hold in $\mathbb{R}$ with 0^* playing the role of 0. (This is step four of Dedekind's construction).

We must verify that the addition of cuts respects the field axioms. In Homework 6, we already showed that cuts are closed under addition which proves axiom $A1$. Let us now show that the addition of cuts satisfies axioms $A2 - A5$.

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 $r + s$ 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 addition of sets, $\beta + \alpha$ refers to the set of all elements $s + r$. However, s and r are elements of $\mathbb{Q}$ and so these elements commute. This means we have $r + s = s + r$ 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 addition of cuts is associative requires the same strategy as above. Namely, we want to show that $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ where α, β, and γ are cuts. Let $r \in \alpha$, $s \in \gamma$, and $t \in \gamma$. Then the element $r + (s + t) \in \alpha + (\beta + \gamma)$. However, since r, s, and t are in $\mathbb{Q}$, then we have $r + (s + t) = (r + s) + t \in (\alpha + \beta) + \gamma$. This holds for all such r, s, and t since these elements are arbitrary which tells us $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

Axiom $A4$ requires us to show that there exists an additive identity. I claim that the additive identity in the set is 0^*. By the previous homework, it is clear that 0^* is a cut. Recall that 0^* refers to the set of all negative rationals. Our objective is to show $\alpha + 0^* = \alpha$. 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 $\alpha + 0^* \subseteq \alpha$. Let $r \in \alpha$ and $s \in 0^*$. Then by the definition of 0^*, we have $r + s < r$. This tells is that $r + s \in \alpha$ which implies $\alpha + 0^* \subseteq \alpha$.
We would now like to show the other inclusion is true, namely $\alpha \subseteq \alpha + 0^*$. Let $p \in \alpha$. We know there exists an $r \in \alpha$ such that $r > p$ by the definition of cuts. Then, $p - r \in 0^*$. This tells us that, $p = r + (p - r) \in \alpha + 0^*$. So we have $\alpha \subseteq \alpha + 0^*$. Since $\alpha + 0^* \subseteq \alpha$ and

$\alpha \subseteq \alpha + 0^*$, we have that $\alpha = \alpha + 0^*$.

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 $\alpha + \beta = 0^*$. Let $z \notin \alpha$. Define β to be the following set: $\beta = \{b \mid b < -z\}$. The first question we have to ask ourselves is how do we know that $\beta \in \mathbb{R}$? That is, how we know that β is a cut?

We first prove that β is not empty. Since $\exists z \notin \alpha$, then β contains all rationals less than $-z$ so β is not empty.

We also know that β does not equal $\mathbb{Q}$. To see this, choose any $a \in \alpha$ and any x such that $x > -a$. Since $z \notin \alpha$, and $a \in \alpha$, this implies that $a < z$, so $-z < -a$. We also have the condition that $x > -a$ which implies that $-z < -a < x$. Since this holds for all such $z \notin \alpha$, then $x \notin \beta$ because the elements of β are less than $-z$. Thus, $\beta \neq \mathbb{Q}$.

We now show that property two of the definition of cut holds. Suppose $b \in \beta$ and let $b' < b$. We must show that $b' \in \beta$. Note that our definition of β tells us that there is some $z \notin \alpha$ such that $b < -z$. But since $b' < b < -z$, it follows that $b' \in \beta$.

Lastly, we must show that β contains no maximal element. Suppose $a \in \alpha$ and $b \in \beta$, where $b < -z$ for some $z \notin \alpha$. From a previous homework, we know that the rationals are dense in the rationals and thus, there exists a b' such that $b < b' < z$ which shows us that $b' \in \beta$.

Now that we know that β is a cut, we must show that $\alpha + \beta = 0^*$. Since these elements are sets, we must show a double inclusion. We will first show that $\alpha + \beta \subseteq 0^*$.

Take $a \in \alpha$, $b \in \beta$ where $b < -z$ for some $z \notin \alpha$. Then, adding a to both sides of the inequality yields: $a + b < a - z$. Note that we also have $a - z < 0$ since $z > a$ because $z \notin \alpha$ while $a \in \alpha$. So we have $a + b < a - z < 0$. This tells us that $\alpha + \beta \subseteq 0^*$.

Next, suppose $c \in 0^*$, so $c < 0$. Choose any $a \in \alpha$ and $z \notin \alpha$ such that $z - a < -c$. Again, since $a < z$, we have $0 < z - a < -c$. Rearranging, we get the following: $c - a < -z$. This shows that $c - a \in \beta$. Note that $c = a + (c - a)$ so $c \in \alpha + \beta$ which shows $0^* \subseteq \alpha + \beta$ since 0^* contains all negative rationals. Thus, these two sets are subsets of each other and hence equal.

Problem 2

Verify that the statement involving addition in Definition 1.17 holds in $\mathbb{R}$. (This is step five in Dedekind's construction).

We would like to show that if $\alpha + \beta + \gamma \in \mathbb{R}$ and $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$. Let $a \in \alpha$, $b \in \beta$, and $c \in \gamma$. By assumption, $\beta < \gamma$ so we have $b < c$ for all $b \in \beta$ and for all $c \in \gamma$. Since a, b and c are in $\mathbb{Q}$, and we already proved that if $b < c$ then $a + b < a + c$, this shows that $\alpha + \beta < \alpha + \gamma$.

Problem 3

Prove that the set of all integers is countable.

Recall that a set is called countable if there exists a 1-1 correspondence between that set and the set of natural numbers. Let $\phi : \mathbb{N} \to \mathbb{Z}$ be defined as follows:

$$\phi(n) = \begin{cases} \dfrac{n}{2}, & \text{if } n \text{ is even} \\ -\dfrac{n-1}{2}, & \text{if } n \text{ is odd} \end{cases}$$

We must show that the function is injective and surjective. It is obvious that the function is surjective, since given any integer, the parity (is an integer even or odd) is unambiguous. The only thing we must do is check if the function is one to one. Assume $\phi(n) = \phi(m)$. We would like to show that $n = m$. Assume n and m are even. Then we have $n/2 = m/2$ so $2n = 2m$ and thus $n = m$. However, it is also possible that n and m are odd. So assume n and m are both odd. Then $-(n-1)/2 = -(m-1)/2$. This implies that $-2(n-1) = -2(m-1)$ and so $n - 1 = m - 1$ which proves that $n = m$. So the function is bijective.

Problem 4

Let $A \sim \mathbb{N}$. Show that if $B \subset A$, then B is at most countable.

We must prove that a subset of a countable set is at most countable. Since $A \sim \mathbb{N}$, there exists a bijection, $f : A \to \mathbb{N}$. Let $g : B \to A$ and define g as follows: $g(b) = \{b\}$. Note this map is valid since $B \subset A$. Also note that g is clearly one to one. Consider the following composition of functions: $f \circ g$. Then we have $f \circ g : B \to \mathbb{N}$. First we will show that $f \circ g$ is one to one.

$$f(g(x)) = f(g(y))$$
$$g(x) = g(y)$$
$$x = y$$

where going from the first line to the second line follows from the fact that f is injective and going from the second line to the third line follows from the fact that g is injective. So we have an injective map from B to $\mathbb{N}$. There are two possibilities for this mapping. Either the mapping is surjective or not surjective. If the mapping is surjective, then we have shown that $B \sim \mathbb{N}$ and so B is countable. If the mapping is not surjective then we still have an injective function whose range is a subset of N and thus $B \sim \mathbb{N}_k$ where $\mathbb{N}_k$ denotes the set $\{1, 2, 3, 4, \ldots, k\}$. This tells us that the set is finite. Thus we may conclude that either B is finite or countably infinite and so we have shown that B is at the most countable.

Prove that the geometric argument presented in class shows that $\mathbb{Q}$ is countable.

Let us first show that $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$. First note that $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. To see the first equivalence relation, let $g : \mathbb{Z} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be specified as follows: $g(x, y) = (\phi^{-1}(x), y)$ where ϕ is defined as in problem 3. We know that ϕ^{-1} exists since ϕ is bijective. Clearly g is bijective since ϕ^{-1} itself is bijective, and the second component in the ordered pair always maps to itself. Now that we know $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N}$, we will show that $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Let $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be specified by $h(m, n) = 2^{m-1}(2n - 1)$. We must prove that h is a bijection. To do this, we will first show injectivity. Assume $h(m, n) = h(a, b)$ - that is, $2^{m-1}(2n - 1) = 2^{a-1}(2b - 1)$. Now either $m > a$, $m < a$, or $m = a$. If $m < a$, then we see that $2n - 1 = 2^{a-m}(2b - 1)$. But the left hand side is an odd integer and the right hand side is an even integer so we have a contradiction. Similarly, if $m > a$, we reach another contradiction of parity. Thus $a = m$. Since $a = m$, this yields $2n - 1 = 2b - 1$ which shows that $n = b$ and thus h is injective.

To show that h is surjective, it suffices to use the Fundamental Theorem of Arithmetic. Since the Fundamental Theorem of Arithmetic (FTOA) holds for natural numbers greater than 2, it should be noted that the number 1 can be obtained from the function h by setting $m = n = 1$. So to show that h is surjective, we must show that any integer greater than or equal to 2 can be obtained from h. Note that for any integer $s \geq 2$ there are three possibilities as a result of the FTOA. Either 2 is the only prime in the prime factorization of s, or there are no factors of 2 in the prime factorization of s or the prime factorization of s has a factor of 2 and a factor which is not 2. Throughout these three cases, we let j denote the number of factors of 2 which appears in the prime factorization.

Case One: Assume that 2 is the only prime in the factorization of s. Choose $n = 1$. Then $s = 2^j = 2^{m-1} * 1 = h(m, n)$.
Case Two: Assume that there are no factors of 2 in the prime factorization of s. Then $j = 0$, so $m = 1$. Since there are no 2's, we know that s must be odd so there exists a $n \in \mathbb{N}$ such that $s = 2n - 1$ by definition of odd numbers. Thus $s = 2n - 1 = 2^0(2n - 1) = h(m, n)$.
Case Three: Assume the prime factorization of s has factors 2 and factors which are not 2. Let t denote the product of the odd primes in the prime factorization of s. Then t is odd so there exists an $n \in \mathbb{N}$ such that $t = 2n - 1$. Thus $s = 2^j t = 2^{m-1}(2n - 1) = h(m, n)$.

Thus the function h is surjective.

Now that we know h is a bijection, we may conclude that $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. Since $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N}$,

it follows that $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$.

Let us now show that $\mathbb{Q} \sim \mathbb{Z} \times \mathbb{N}$. Let us define $\mathbb{Q}$ as follows:
$\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, \ q \in \mathbb{N}, \ gcd(p, q) = 1\}$. Now from the diagram in class, it is natural to let
$f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ be defined by $f(p/q) = (p, q)$. f is one to one since if $f(m/n) = f(p/q)$, then
$(m, n) = (p, q)$ and so $m = n$ and $q = p$. From above, we know that $\mathbb{Z} \times \mathbb{N}$ is countable -
that is, there exists a bijection $\psi : \mathbb{Z} \times \mathbb{N} \to \mathbb{N}$. Since f and ψ are injective, then we have
$\psi \circ f : \mathbb{Q} \to \mathbb{N}$ is also an injective function (see Problem 4). I claim that this is enough
to show that $\mathbb{Q}$ is a countable set. To see this, note that $\psi(f(\mathbb{Q}))$ is a nonempty subset
of $\mathbb{N}$. Then by problem 4, since $\mathbb{N} \sim \mathbb{N}$, and $\psi(f(\mathbb{Q})) \subset \mathbb{N}$, it follows that $\psi(f(\mathbb{Q}))$ is at
most countable. However, $\psi(f(\mathbb{Q}))$ is infinite which tells us that $\psi(f(\mathbb{Q}))$ is countable, so
$\psi(f(\mathbb{Q})) \sim \mathbb{N}$. Due to the function being injective, $\mathbb{Q} \sim \psi(f(\mathbb{Q}))$. Since $\psi(f(\mathbb{Q})) \sim \mathbb{N}$, it
therefore follows that $\mathbb{Q} \sim \mathbb{N}$ by transitivity of this equivalence relation.

Problem 6

Give an example of a field which is an ordered set, but is not an ordered field.

I claim once we have a field with an order, then that field is automatically an ordered
field. To see this let F be a field and let an order on F be denoted by $<$. We would like to
show that F has the following two properties of ordered fields:

(a) If $x, y, z \in F$, and $y < z$, then $x + y < x + z$.

(b) If $x, y \in F$, and $x > 0$, and $y > 0$, then $xy > 0$.

Since F has an order, it is clear that there exists elements x and y such that $x < y$. [It
should be noted that no finite field can be ordered. To see this, assume there exists a finite
field with an order. By our axioms and a homework exercise, we know that in whatever field
this is, $0 < 1$. Since the field is closed, $0 + 1 < 1 + 1$. Similarly, $0 + 1 + 1 < 1 + 1 + 1$.
Repeating this argument indefinitely tells us that the field has infinitely many elements]. By
the closure of the field, we know there exists a positive element a such that $x + a = y$. Then,
adding z to both sides yields $x + a + z = y + z$. Since a is a positive element of the field, we
have $x + z < y + z$.

Now we want to show that if $x, y \in F$, and $x > 0$ and $y > 0$, then $xy > 0$. We will prove this
by contradiction. If $xy \leq 0$, it is clear that the case $xy = 0$ leads to a contradiction since
Proposition 1.16 (a) shows that either

(a) $x = 0$ or $y = 0$

(b) $x = y = 0$

We must only show that $xy < 0$ is false. Since this statement holds for all x and for all
y, then take $x = 1 = y$. Then we get $1 < 0$ which contradicts the result from a previous
homework which shows that in any field, $1 > 0$.