Homework 2 (due Mar. 7)

손량(20220323)

Last compiled on: Tuesday 7th March, 2023, 16:45

1 Problem 6

1.1 Solution for (a)

If $m = 0$ and $p = 0$, $b^m = b^p = 1$ and the equality holds. Let's prove for $m, p \neq 0$ case.

Let $x := (b^m)^{1/n}, y := (b^p)^{1/q}$. We can obtain

$$x^{np} = (x^n)^p = (b^m)^p = b^{mp}, \quad y^{mq} = (y^q)^m = (b^p)^m = b^{mp}$$

x, y can be written as follows, by the theorem 1.21 in the book.

$$x = (b^{mp})^{1/(np)}, \quad y = (b^{mp})^{1/(mq)}$$

Since $np = mq$, $x = (b^{mp})^{1/(np)} = (b^{mp})^{1/(mq)} = y$ holds.

1.2 Solution for (b)

Let $r := m/n, s = p/q$. b^{r+s} can be written as:

$$b^{r+s} = b^{(mq+np)/(nq)} = (b^{mq+np})^{1/(nq)}$$

By corollary of theorem 1.21,

$$(b^{mq}b^{np})^{1/(nq)} = (b^{mq})^{1/(nq)}(b^{np})^{1/(nq)}$$

Using the fact we proved in (a),

$$(b^{mq})^{1/(nq)}(b^{np})^{1/(nq)} = (b^m)^{1/n}(b^p)^{1/q} = b^r b^s$$

1.3 Solution for (c)

First, let's show that b^r is an upper bound of $B(r)$. Suppose that there exists an element b^u such that $u \leq r$ and $b^u > b^r$. Using the result from (b),

$$b^r = b^{r-u+u} = b^{r-u}b^u < b^u$$

If we write $u = m/n$ for integers m and n, it can be shown that $b^u = (b^m)^{1/n} > 0$ using the theorem 1.21 in the book and the fact that $b^m > 0$. Thus, $b^{r-u} < 1$ should hold. Since $r \geq u$, $r - u$ can be written as p/q where p is a nonnegative integer, and q is a positive integer. Then $b^{r-u} = (b^p)^{1/q} > 0$, so $0 < (b^p)^{1/q} < 1$ implies $b^p < 1$. However, since $b > 1$, it implies $b^p \geq 1$ for nonnegative integer p, which is a contradiction. Thus, b^u cannot exist.

Since $B(r)$ is a set of reals with an upper bound, it has the least upper bound, $\sup B(r)$. Suppose that there exists b^v where v is rational, such that $b^v < b^r$ and $b^v \geq y \; \forall y \in B(r)$. It is evident that such b^v cannot exist since b^r is also an element of $B(r)$. In conclusion, upper bound smaller than b^r cannot exist and $b^r = \sup B(r)$.

1.4 Solution for (d)

First, let's show that $\sup B(x) \sup B(y)$ is an upper bound of $B(x+y)$. For all elements in $b^t \in B(x+y)$ where $t \leq x+y$ is a rational, there are two possibilities:

1. $t < x+y$
2. $t = x+y$

If there exists an element b^t such that $t = x+y$, $x+y$ is a rational so $\sup B(x+y) = b^{x+y}$ as we proved in (c).

Let's consider the case where $t < x+y$ holds for all $b^t \in B(x+y)$. There exists a rational r such that $t - y < r < x$ by theorem 1.20. Then, we can let $s := t - r$ and $s < y$ holds. In other words, t can be written as $r + s$ where r, s are rationals such that $r < x$ and $s < y$. As proven in (b), $b^t = b^{r+s} = b^r b^s$ and $b^r \in B(x), b^s \in B(y)$ holds. By the definition in (c), $b^r \leq \sup B(x) = b^x$ and $b^s \leq \sup B(y) = b^y$. This implies that for all $b^t \in B(x+y)$,

$$b^t = b^{r+s} = b^r b^s \leq \sup B(x) \sup B(y)$$

Thus, $\sup B(x) \sup B(y)$ is an upper bound of $B(x+y)$. Now we have to show that $\sup B(x+y) = \sup B(x) \sup B(y)$. Suppose that there exists an upper bound of $B(x+y)$ that is smaller than $\sup B(x) \sup B(y)$ and call it c. The following holds:

$$\frac{c}{\sup B(x)} < \sup B(y)$$

Since $\sup B(y)$ is the least upper bound of $B(y)$, there exists $b^v \in B(y)$ such that $c / \sup B(x) < b^v \leq \sup B(y)$.[1] Now, the following holds since $\sup B(x), b^v > 0$:

$$\frac{c}{b^v} < \sup B(x)$$

There exists $b^u \in B(x)$ such that $c/b^v < b^u \leq \sup B(x)$. Now, we get $c < b^u b^v$ and $b^u b^v \in B(x+y)$ which is a contradiction. Such lower bound c does not exist, so $b^x b^y = \sup B(x) \sup B(y) = \sup B(x+y) = b^{x+y}$.

2 Problem 7

2.1 Solution for (a)

$b^n - 1$ can be written as follows:

$$b^n - 1 = (b-1)(b^{n-1} + b^{n-2} + \cdots + b + 1)$$

Since $b > 1$, we know $b^{n-1} > b^{n-2} > \cdots > b > 1$. The polynomial $b^{n-1} + b^{n-2} + \cdots + b + 1$ has n terms, and each term is greater or equal to 1. So we get

[1] If such b^v did not exist, then $\sup B(y)$ cannot be the least upper bound of $B(y)$.

$$b^i \geq 1 \ (i = 0, 1, \ldots, n-1) \Longrightarrow b^{n-1} + b^{n-2} + \cdots + b + 1 \geq n$$

And we obtain the inequality $b^n - 1 \geq n(b-1)$.

2.2 Solution for (b)

Let $c := b^{1/n}$. By theorem 1.21, $c > 0$. Suppose that $c \leq 1$. Then $1 \geq c \geq c^2 \geq \cdots \geq c^n = (b^{1/n})^n = b$, and it is a contradiction. Hence, $c > 1$. Plugging c to the inequality we obtained in (a), we get

$$c^n - 1 \geq n(c-1) \Longrightarrow b - 1 \geq n(b^{1/n} - 1)$$

2.3 Solution for (c)

Since $t > 1$, $n > (b-1)/(t-1)$ can be written as $n(t-1) > b-1$. By the inequality from (b), we can write

$$n(t-1) > b - 1 \geq n(b^{1/n} - 1)$$

Since n is positive, $b^{1/n} < t$ holds.

2.4 Solution for (d)

Since $b > 0$, $b^w > 0$ and $t := y \cdot b^{-w} > 1$ holds by the definition we made in problem 6(c). By the archimedean property, there exists a positive interger n such that $n(t-1) > b-1$. From the result from (c), $b^{1/n} < t = y \cdot b^{-w}$ and $b^{w+(1/n)} < y$ holds for a sufficiently large integer n.

2.5 Solution for (e)

Since $y > 0$, $t := b^w/y > 1$ holds. By the archimedean property, there exists a positive integer n such that $n(t-1) > b-1$. From the result from (c), $b^{1/n} < t = b^w/y$ and $b^{w-(1/n)} > y$ holds for a sufficiently large integer n.

2.6 Solution for (f)

Suppose that $b^x > y$. By the result from (e), there exists a positive integer n such that $b^{x-(1/n)} > y$. This means that $x - (1/n)$ is also an upper bound of A, and since $b^{x-(1/n)} < b^x$, it is a contradiction. Thus, $b^x \leq y$ holds.

Suppose that $b^x < y$. By the result from (d), there exists a positive integer n such that $b^{x+(1/n)} < y$. This means that x cannot be an upper bound of A, because there exists an $b^{x+(1/n)}$ is also an element of A. Thus, $b^x \geq y$ holds. In conclusion, b^x should satisfy both $b^x \leq y$ and $b^x \geq y$, so $b^x = y$.

2.7 Solution for (g)

Suppose that there exists a real $z \neq x$ such that $b^z = y$. There are two possibilities:

1. $z > x$

2. $z < x$

In $z > x$ case, $b^z = b^{z-x+x} = b^{z-x}b^x > b^x = y$, so it is a contradiction.[2]

In $z < x$ case, $b^x = b^{x-z+z} = b^{x-z}b^z > b^z = y$, so it is also a contradiction. In conclusion, such z cannot exist and thus x is unique.

3 Problem 8

Suppose that a relation $<$ is defined for complex field, and it satsifies all axioms for ordered field. Then, one of the statements is true.

$$i < 0, \quad i = 0, \quad i > 0$$

$i = 0$ is impossible because $i \cdot i = -1 \neq 0$, by definition.

If $i < 0$, we can multiply both sides with i and obtain $-1 > 0$. Multiplying both sides with i agian, we obtain $-i < 0$, which contradicts with $i < 0$.

If $i > 0$, the same operations can be done like the $i < 0$ case, and we obtain $-i > 0$, which also contradicts with $i > 0$. In conclusion, the assumed relation $<$ cannot exist.

4 Problem 20

4.1 Proof for the least-upper-bound property

Let A be a nonempty subset of $\mathbb{R}$ and assume that $\beta \in \mathbb{R}$ is an upper bound of A. Define γ as the union of all $\alpha \in A$. In other words, $p \in \gamma$ if and only if $p \in \alpha$ for some $\alpha \in A$. Let's prove that $\gamma \in \mathbb{R}$ and $y = \sup A$.

Since A is nonempty, there exists a nonempty $\alpha_0 \in A$. From $\alpha_0 \subset \gamma$, γ is not empty. For all $\alpha \in A$, $\alpha \subset \beta$. This means $\gamma \subset \beta$ and $\gamma \neq \mathbb{Q}$, so γ satsifies property (I). To prove (II), pick $p \in \gamma$ and we can see that $p \in \alpha_1$ for some $\alpha_1 \in A$. If $q < p$, then $q \in \alpha_1$ and $q \in \gamma$ holds, proving (II). Thus $\gamma \in \mathbb{R}$ and $\alpha \leq \gamma$ by the definition of γ, so γ is an upper bound of A.

Now, suppose that $\delta < \gamma$ where δ is also an upper bound of A. Then there exists $s \in \gamma$ such that $s \neq \delta$. Since $s \in \gamma$, $s \in \alpha$ for some $\alpha \in A$, so $\delta \geq \alpha$ is impossible. In conclusion, such upper bound δ cannot exist, so we get the desired result: $\gamma = \sup A$.

4.2 Proof for addition axioms

Define 0^* to be the set of all nonpositive rational numbers. 0^* is a cut because it satisfies property (I) and (II).

4.2.1 Proof for (A1)

For all $\alpha, \beta \in \mathbb{R}$, the sum of two cuts $\alpha + \beta$ is a nonempty subset of $\mathbb{Q}$ by the definition of addition. Take $r' \notin \alpha, s' \notin \beta$, and $r' + s' > r + s$ for all $r \in \alpha, s \in \beta$ holds as $\mathbb{Q}$ is an ordered field. Thus $r' + s' \notin \alpha + \beta$ and $\alpha + \beta \neq \mathbb{Q}$, so $\alpha + \beta$ satisfies property (I).

For $p \in \alpha + \beta$, then $p = r + s$ where $r \in \alpha, s \in \beta$. If $q < p$, $q - s < p - s = r$ holds, so $q - s \in \alpha$ and $q = (q - s) + s \in \alpha + \beta$. Thus property (II) holds and $\alpha + \beta$ is a cut.

[2]In general, $b^w > 0$ where $w > 0, b > 1$ holds because a positive rational $r = m/n$ exists with $0 < r < w$ and $b^r = (b^m)^{1/n}$. Then $b^m > 1$ and $b^r = (b^m)^{1/n} > 1$ holds. By the definition we made in problem 6(c), $b^w \geq b^r > 1$.

4.2.2 Proof for (A2)

By definition, for all $\alpha, \beta \in \mathbb{R}$, $\alpha + \beta$ is the set of all $r + s$ where $r \in \alpha, s \in \beta$. Similarly, $\beta + \alpha$ is the set of all $s + r$, and $r + s = s + r$ for all $r \in \alpha, s \in \beta$ as $\mathbb{Q}$ is a field. So $\alpha + \beta = \beta + \alpha$ holds.

4.2.3 Proof for (A3)

Similar to the proof for (A2), for all $\alpha, \beta, \gamma \in \mathbb{R}$, $(\alpha+\beta)+\gamma$ is the set of all $(r+s)+t$ where $r \in \alpha, s \in \beta, t \in \gamma$. Likewise, $\alpha+(\beta+\gamma)$ is the set of all $r+(s+t)$, and $r+(s+t) = (r+s)+t$ for all $r \in \alpha, s \in \beta, t \in \gamma$ as $\mathbb{Q}$ is a field. Thus, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ holds.

4.2.4 Proof for (A4)

For $r \in \alpha$ and $s \in 0^*$, $r + s \leq r$, so $r + s \in \alpha$ and $\alpha + 0^* \subset \alpha$ holds.

For all $p, r \in \alpha$ where $r \geq p$, $p - r \in 0^*$ and $p = r + (p - r) \in \alpha + 0^*$ holds. Thus $\alpha \subset \alpha + 0^*$ and we obtain the desired result: $\alpha + 0^* = \alpha$.

4.2.5 Proof for failure of (A5)

Suppose that (A5) holds in this particular construction of $\mathbb{R}$. Let α be a set of negative rationals, then α is a cut by definition, and $\beta \in \mathbb{R}$ such that $\alpha + \beta = 0^*$ exists. From $0 \in 0^* \subset \alpha + \beta$, $0 \in \alpha + \beta$ holds. By the definition of addition, there exists $r \in \alpha, s \in \beta$ such that $r+s = 0$. Since $r < 0$ for all $r \in \alpha$, there exists $s' \in \beta$ such that $s' > 0$. However, $-s'/2 \in \alpha$ by definition, and $-s'/2 + s' = s'/2 \in \alpha + \beta = 0^*$, but it is a contradiction because $s'/2 > 0$. Thus, this particular construction of $\mathbb{R}$ without property (III) of cuts cannot satisfy the axiom (A5).