18.100B: Problem Set 1

Dmitry Kaysin

October 2019

Problem 1

Prove that there is no rational number whose square is 12.

Proof. Suppose there exist $p, q \in \mathbb{Z}$ such that p and q are relatively prime and $\left(\frac{p}{q}\right)^2 = 12$.

$$p^2 = (4)(3)q^2$$

This means that 3 divides p^2, which is only possible if 3 divides p, or $p = 3k$.

$$p^2 = 9k^2 = (4)(3)q^2$$

$$3k^2 = 4q^2$$

This means that 3 divides q^2 and 3 divides q. We've arrived at conclusion that 3 divides both p and q, a contradiction to the assumption that p and q are relatively prime. Thus, there is no rational number whose square is 12.

□

Problem 2

Let S be a non-empty subset of the real numbers, bounded above. Show that if $u = \sup S$, then for every natural number n, the number $u - \frac{1}{n}$ is not an upper bound of S, but the number $u + \frac{1}{n}$ is an upper bound of S.

Proof. If u is the least upper bound of S then no upper bound of S is larger than u. Suppose $u - \frac{1}{n}$ is an upper bound of S. But $u - \frac{1}{n} < u$. Then u cannot be the least upper bound. Contradiction.

Since u is the least upper bound of S then $s \leq u$ for all $s \in S$. Therefore $s \leq u < u + \frac{1}{n}$ for any $n \in \mathbb{N}$ and $u + \frac{1}{n}$ is an upper bound of S by definition.

□

Problem 3

Show that if A and B are bounded subsets of $\mathbb{R}$, then $A \cup B$ is a bounded subset of $\mathbb{R}$. Show that

$$\sup A \cup B = \max(\sup A, \sup B)$$

Proof. If A and B are bounded subsets of $\mathbb{R}$ then there exist real numbers $\sup A$ and $\sup B$. Let $x = \max(\sup A, \sup B)$.

$$\forall a \in A : a \leq \sup A \leq x$$

$$\forall b \in B : b \leq \sup B \leq x$$

Therefore:

$$\forall c \in A \cup B : c \leq x$$

Thus, x is an upper bound of $A \cup B$. The same argument applies for the greatest lower bounds of A and B. Thus, $A \cup B$ is bounded.

Now we prove that x is the least upper bound. Suppose that there is another upper bound of $A \cup B$, namely y, such that $y < x$. Then y must be an upper bound for both sets A and B. Otherwise there would be an element t in one of the sets A or B and, consequently, $A \cup B$, such that $t > y$. But this is impossible since x is the least upper bound for at least one of the sets A or B. Thus, $x = \max(\sup A, \sup B)$ is the least upper bound of the combined set $A \cup B$.

□

Problem 4

Fix $b > 1$.
a) If m, n, p, q are integers, $n > 0$, $q > 0$, and $r = m/n = p/q$, prove that

$$(b^m)^{\frac{1}{n}} = (b^p)^{\frac{1}{q}} \tag{1}$$

Proof. We raise LHS and RHS of the expression 1 into nq-th power:

$$((b^m)^{\frac{1}{n}})^{nq} = b^{mq}$$

$$((b^p)^{\frac{1}{q}})^{nq} = b^{pn}$$

Notice that $\frac{m}{n} = \frac{p}{q} \Rightarrow pn = mq$. Hence, $b^{mq} = b^{pn}$.

We claim that if $a^n = b^n$ where $n \in \mathbb{Z}$, then $a = b$ by induction. This claim is true for $n = 1$:

$$a^1 = b^1 \Rightarrow a = b$$

For arbitrary $n \in \mathbb{N}$ we prove that $a^n = b^n$ if $a^{n-1} = b^{n-1}$:

$$\begin{aligned} a^n &= b^n \\ ab^{-1}a^{n-1} &= b^{n-1} \\ ab^{-1} &= 1 \\ a &= b \end{aligned}$$

Note that the claim is not true for $n = 0$ since $a^0 = 1$ is always equal to $b^0 = 1$.

For negative integer powers the claim is also true. Consider $n \in \mathbb{Z}, n < 0$. Assume $a^{-n} = b^{-n}$, then:

$$\frac{1}{a^n} = \frac{1}{b^n} \Rightarrow a^n = b^n \Rightarrow a = b$$

Going back to our example, nq is an integer (product of two integers), therefore:

$$(b^m)^{\frac{1}{n}} = (b^p)^{\frac{1}{q}}$$

This means that there is only one rational number b^r for $b > 1$ and any given rational number r.

□

b) Prove that $b^{r+s} = b^r b^s$ if r, s are rational.

Proof. We know that $b^r + b^s = b^{r+s}$ for $r, s \in \mathbb{Z}$. We now prove that this is also the case for $r, s \in \mathbb{Q}$. Let $r = \frac{p}{q}$ and $s = \frac{m}{n}$. We raise LHS and RHS of the expression to the qn-th power:

$$\begin{aligned} &\text{LHS: } (b^{\frac{p}{q}+\frac{m}{n}})^{qn} = (b^{\frac{pn+mq}{qn}})^{qn} = b^{pn+mq} \\ &\text{RHS: } (b^{\frac{p}{q}} b^{\frac{m}{n}})^{qn} = ((b^p)^{\frac{1}{q}} (b^m)^{\frac{1}{n}})^{qn} = b^{pn} b^{mq} = b^{pn+mq} \end{aligned}$$

LHS is equivalent to RHS, hence $(b^{r+s})^{qn} = (b^r b^s)^{qn}$ where $r, s \in \mathbb{Q}$ and qn is integer. Therefore $b^{r+s} = b^r b^s$.

□

c) If x is real, define $B(x)$ to be the set of all numbers b^t, where t is rational and $t \leq x$. Prove that

$$b^r = \sup B(r)$$

when r is rational.

Proof. First we prove that for $b > 1 : t \leq r \Rightarrow b^t \leq b^r$. We note that $(b^n)^{-1} = \frac{1}{b^n} = b^{-n}$ for $n \in \mathbb{Q}$. Then $b^m \leq b^n \iff b^n b^{-m} \geq 1 \iff b^{n-m} \geq 1$. We can see that $n - m$ is a rational number. Let it be equal to $\frac{p}{q}$. Then $b^{n-m} = (b^p)^{\frac{1}{q}}$ is larger than or equal to 1 as long as $n - m \geq 0$ (with equality being satisfied when $n = m$). Thus, $n - m \geq 0 \iff m \leq n \iff b^m \leq b^n$ for $b > 1$. In other words, $f : t \mapsto b^t$ is a monotone (order preserving) map for $r \in \mathbb{Q}$.

Denote $R(r) = \{t \mid t \in \mathbb{Q}, t \leq r\}$, all rational numbers less than or equal to r. The monotone map f maps the largest element of $R(r)$ to the largest element of $B(r)$, or $\forall t \in R(r) : b^t \leq b^r$. Since all elements of $B(r)$ are less or equal to b^r, then it is an upper bound for $B(r)$. Since b^r is an element of $B(r)$, it is the least upper bound.

□

d) Prove that $b^{x+y} = b^x b^y$ for all real x and y.

Proof. For all $m \in R(x)$ and $n \in R(y)$ (m and n are rational) the following holds by (b):

$$b^{m+n} = b^m b^n$$

Since map $t \mapsto b^t$ is monotone for $b > 1$, $\forall m \in R(x) : b^m \leq \sup B(x)$ and $\forall n \in R(y) : b^n \leq \sup B(y)$:

$$b^{m+n} \leq \sup B(x) \sup B(y)$$

By definition $b^x = \sup B(x)$ and $b^y = \sup B(y)$, then:

$$\forall m \in R(x), \forall n \in R(y) : b^{m+n} \leq b^x b^y$$

We note that $x = \sup R(x)$ and $y = \sup R(y)$ by definition. Then $\sup\{m + n \mid m \in R(x), n \in R(y)\} = x + y$, and:

$$\forall t \in B(x + y) : t \leq b^x b^y$$

Thus, $b^x b^y$ is an upper bound for $B(x+y)$. We now prove that it is the least upper bound. Suppose there exists $r \in \mathbb{R}$, such that r is an upper bound for $B(x + y)$ and $r < b^x b^y$. Then, since $\mathbb{Q}$ is dense in $\mathbb{R}$, there must exist rational $p \in R(x)$ and $q \in R(y)$ such that $r < b^p b^q < b^x b^y$. Then $r < b^p b^q = b^{p+q} \in B(x + y)$. Thus, r cannot be an upper bound for $B(x + y)$. Contradiction.

Thus, $b^x b^y$ is the least upper bound for $B(x + y)$, or:

$$b^{x+y} = b^x b^y$$

□

Problem 5

Prove that no order can be defined in the complex field that turns it into an ordered field.

Proof. Suppose there exists an order that turns $\mathbb{C}$ into an ordered field. Then, the following must hold for any ordered field:

$$\forall a \in \mathbb{F} : a^2 \geq 0$$

Note that -1 cannot be equal to 0 since only one distinct additive identity is possible in a field. Thus:

$$-1 = i^2 > 0$$

The following must also hold for any ordered field:

$$a > 0 \iff -a < 0$$
$$-1 > 0 \iff 1 < 0$$

However the following must also hold:

$$1 = (-1)^2 > 0$$

Contradiction. Thus, no order can be defined in the complex field that turns it into an ordered field.

□

Problem 6

Suppose $z = a + bi$, $w = c + di$. Define $z < w$ if $a < c$ or $a = c, b < d$. Prove that this turns the set of all complex numbers into an ordered set. (This is known as a dictionary order, or lexicographic order)

Proof. Consider $z = a+bi$, $w = c+di$. We can see that only one of the following can be true: $z < w$, $z > w$ or $z = w$:

- If $a > c$ then $z > w, z \neq w, z \not< w$;
- If $a < c$ then $z < w, z \neq w, z \not> w$;
- if $a = c$ and $b = d$ then $z \not> w, z = w, z \not< w$;
- If $a = c$ and $b > d$ then $z > w, z \neq w, z \not< w$
- if $a = c$ and $b < d$ then $z \not> w, z \neq w, z < w$

Consider $z = a + bi$, $w = c + di$, $u = e + fi$, such that $z < w, w < u$. Since $z < w$ then either $a < c$ or $a = c, b < d$. Since $w < u$ then either $c < e$ or $c = e, d < f$. Transitivity of the given order ($z < u$) follows from transitivity of standard ordering of real numbers a, b, c, d, e, f.

□

Does this ordered set have the least-upper-bound property?

Answer: No.

Proof. Consider the set $E(x) = \{a + bi \mid a < x, b \in \mathbb{R}\}$ with the given order. All upper bounds of set $E(x)$ are $U = \{a + bi \mid a \geq xb \in \mathbb{R}\}$. However, for any upper bound $u = (a + bi) \in U$ there exists an upper bound $g \in U$ such that $g > u$, for example $g = a + (b + d)i$ where $d > 0$. Therefore, no least upper bound exists for $E(x)$.

□

Problem 7

Prove that

$$|x + y|^2 + |x - y|^2 = 2|x|^2 + 2|y|^2 \tag{2}$$

if $x \in \mathbb{R}^k$ and $y \in \mathbb{R}^k$. Interpret this geometrically, as a statement about parallelograms.

Proof. We rewrite the expression using dot product:

$$(x + y) \cdot (x + y) + (x - y) \cdot (x - y) = 2(x \cdot x) + 2(y \cdot y)$$

We apply distributive property over addition:

$$x \cdot x + 2(x \cdot y) + y \cdot y + x \cdot x - 2(x \cdot y) + y \cdot y = 2(x \cdot x) + 2(y \cdot y)$$

$$2(x \cdot x) + 2(y \cdot y) = 2(x \cdot x) + 2(y \cdot y)$$

Thus, the original expression is true.

To interpret this result geometrically, we consider a parallelogram in $\mathbb{R}^2$ with longer side x and with shorter side y. Then $x + y$ is this parallelogram's longer diagonal and $x - y$ is its shorter diagonal. Therefore equality 2 is equivalent to the following observation: the sum of squares of lengths of parallelogram's diagonals is equal to twice the sum of squares of its (distinct) sides.

□