18.100B Problem Set 1 Solutions
Sawyer Tabony

1) The proof is by contradiction. Assume \( \exists r \in \mathbb{Q} \) such that \( r^2 = 12 \). Then we may write \( r \) as \( \frac{a}{b} \) with \( a, b \in \mathbb{Z} \) and we can assume that \( a \) and \( b \) have no common factors. Then

\[
12 = r^2 = \left( \frac{a}{b} \right)^2 = \frac{a^2}{b^2},
\]

so \( 12b^2 = a^2 \).

Notice that 3 divides \( 12b^2 \) and hence 3 divides \( a^2 \). It follows that 3 has to divide \( a \) (one way to see this: every integer can be written as either \( 3n \), \( 3n + 1 \), or \( 3n + 2 \) for some integer \( n \). If you square these three choices, only the first one gives you a multiple of three.)

Let \( a = 3k \), for \( k \in \mathbb{Z} \). Then substitution yields \( 12b^2 = (3k)^2 = 9k^2 \), so dividing by 3 we have \( 4b^2 = 3k^2 \), so 3 divides \( 4b^2 \) and hence 3 divides \( b^2 \). Just as for \( a \), this implies that \( b \) has to divide \( b \). But then \( a \) and \( b \) share the common factor of 3, which contradicts our choice of representation of \( r \). So there is no rational number whose square is 12.

2) \( S \subseteq \mathbb{R}, S \neq \emptyset \), and \( u = \sup S \). Given any \( n \in \mathbb{N}, \forall s \in S, s \leq u < u + \frac{1}{n} \), so \( u + \frac{1}{n} \) is an upper bound for \( S \). Assume \( u - \frac{1}{n} \) is also an upper bound for \( S \). Since \( u - \frac{1}{n} < u \), \( u \) would not be the least upper bound for \( S \), which is a contradiction. Therefore \( u - \frac{1}{n} \) is not an upper bound for \( S \).

3) Recall that a subset of the real numbers, \( A \subseteq \mathbb{R} \), is bounded if there are real numbers \( a \) and \( a' \) such that

\[
t \in A \implies a' \leq t \leq a.
\]

Since \( A, B \subseteq \mathbb{R} \) are bounded, they have upper bounds \( a \) and \( b \) respectively, and lower bounds \( at \) and \( bt \). Let \( \alpha = \max(a, b) \) and \( \beta = \min(at, bt) \). Clearly,

\[
t \in A \implies \beta \leq a' \leq t \leq a \leq \alpha
\]

\[
t \in B \implies \beta \leq b' \leq t \leq b \leq \alpha,
\]

hence any \( t \in A \cup B \) satisfies \( \beta \leq t \leq \alpha \) and \( A \cup B \) is bounded.

Notice that, in particular, this shows that \( \max\{\sup A, \sup B\} \) is an upper bound for \( A \cup B \), so we only have to show that it is the least upper bound. Suppose \( \gamma < \max\{\sup A, \sup B\} \). Then without loss of generality, \( \gamma < \sup A \). By definition of supremum, \( \gamma \) is not an upper bound of \( A \), so \( \exists a \in A \) with \( \gamma < a \). But \( a \in A \Rightarrow a \in A \cup B \), so \( \gamma \) is not an upper bound of \( A \cup B \). Therefore

\[
\max\{\sup A, \sup B\} = \sup A \cup B.
\]

4) Start by noting that, if \( n, m \in \mathbb{N} \) then \( b^n b^m = b^{n+m} \) from which it follows that \( b^n b^m = b^{n+m} \) for \( n, m \in \mathbb{Z} \) (why?). Similarly, you can show that \( b^m = \left( b^n \right)^m \) for \( n, m \in \mathbb{Z} \). Recall that, if \( x > 0 \), then \( x^{\frac{1}{n}} \) is defined to be the unique positive real number such that \( \left( x^{\frac{1}{n}} \right)^n = x \).

a) We have that \( m/n = p/q \) so \( mq = pn \). Notice that \( \left( \left( b^n \right)^{\frac{1}{n}} \right)^m = \left( b^n \right)^q = b^{mq} \) and that

\[
\left( \left( b^n \right)^{\frac{1}{n}} \right)^m = \left( b^n \right)^m = b^{mn},
\]

which is also equal to \( b^{mq} \). But we know that there is a unique real
number $y$ satisfying $y^{nq} = b^{mq}$ hence the two numbers we started with have to be equal, i.e.,

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

Notice that if this equality didn’t hold, then we could not make sense of the symbol $b^r$ for $r \in \mathbb{Q}$, because the value would change if we wrote the same number $r$ in two different ways.

b) Let $r, s \in \mathbb{Q}$ with $r = \frac{m}{n}$ and $s = \frac{p}{q}$. Since $nq$ is an integer we know that

$$(b^r b^s)^{nq} = (b^r)^{nq} (b^s)^{nq}$$

but $(b^r)^{nq} = \left((b^m)^{\frac{1}{n}}\right)^{nq} = (b^m)^{\frac{nq}{n}} = b^{mq}$ and similarly $(b^s)^{nq} = b^{np}$. Since $mq$ and $np$ are integers we can conclude

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

But there is a unique positive real number, $y$, such that $y^{nq} = y^{mq+np}$, so we know that

$b^r b^s = (b^{mq+np})^{\frac{1}{nq}} = b^{\frac{mq+np}{nq}} = b^{\frac{nq}{n} + \frac{nq}{q}} = b^{r+s}.$

c) Now with $b > 1$, given $r, s \in \mathbb{Q}, s \leq r$ we want to show $b^s \leq b^r$. Let $r - s = \frac{m}{n}$, $0 < n, 0 \leq m$ since $s \leq r$. Then $b^{r-s} = (b^m)^{\frac{1}{n}}$, and it is easy to see that $1 \leq b^m$, since $0 \leq m$ and $1 < b$.

Thus a positive power of $b^{r-s}$ is greater than or equal to 1, which implies $1 \leq b^{r-s}$. Multiplying by $b^s$ gives $b^s \leq b^{r-s} b^s = b^{(r-s)+s} = b^r$, so $b^s \leq b^r$. Hence for any $b^s \in B(r)$, $s \leq r \Rightarrow b^s \leq b^r$, so $b^r$ is an upper bound for $B(r)$. Since $b^r \in B(r)$, $b^r$ must be the least upper bound, so $b^r = \sup B(r)$.

d) So let $x, y \in \mathbb{R}$. If $r, s \in \mathbb{Q}$ are such that $r \leq x, s \leq y$, then $r + s \leq x + y$ so $b^{r+s} \in B(x+y)$ and $b^r b^s \leq b^{x+y}$. Keeping $s$ fixed, notice that for any $r \leq x$ we have

$$b^r \leq \frac{b^{r+y}}{b^x},$$

thus $\frac{b^{r+y}}{b^x}$ is an upper bound for $B(x)$ which implies $b^r \leq \frac{b^{r+y}}{b^x}$. We rearrange this to

$$b^s \leq \frac{b^{r+y}}{b^x}$$

and conclude that $b^y \leq \frac{b^{x+y}}{b^x}$ or $b^r b^y \leq b^{x+y}$.

Suppose the inequality is strict. Then $\exists t \in \mathbb{Q}$, $t < x+y$, such that $b^r b^y < b^t \, ^1$. We will find $r, s \in \mathbb{Q}$, with $r \leq x, s \leq y$ and $t < r+s < x+y$. First, find $N \in \mathbb{N}$ so that $N \left(x+y-t\right) > 1$, then find $r \in \mathbb{Q}$ so that $x - \frac{1}{2N} < r < x$ and $s \in \mathbb{Q}$ such that $y - \frac{1}{2N} < s < y$ (the existence of $N, r, s$ follow from the Archimedean property of $\mathbb{R}$ as shown in class). Now, notice that

$$N \left(x+y-t\right) > 1 \implies t < x+y - \frac{1}{N},$$

$$x - \frac{1}{2N} < r < x \text{ and } y - \frac{1}{2N} < s < y \implies x+y - \frac{1}{N} < r+s < x+y$$

hence we have $t < r+s < x+y$ just like we wanted.

\(^1\)This is true even if $x+y \in \mathbb{Q}$, notice that $\sup B(x+y) = \sup \{b^t : t \in \mathbb{Q}, t < x+y\}$
But now we have
\[ b^r b^y < b^t < b^{r+s} = b^r b^y \]
which is a contradiction because, since \( r < x \) and \( s < y \), we have \( b^r < b^x \) and \( b^y < b^y! \) \(^2\)

5) We know that in any ordered field, squares are greater than or equal to zero. Since \( i^2 = -1 \), this means that \( 0 \leq -1 \). But then \( 1 = 0 + 1 \leq -1 + 1 = 0 \leq 1 \) which implies \( 0 = 1 \), a contradiction!

6) I’ll write \( \preccurlyeq \) for this relation on \( \mathbb{C} \) to distinguish it from the normal order on \( \mathbb{R} \). To show that \( \preccurlyeq \) is an order on \( \mathbb{C} \), we must show both transitivity and totality (or given \( x, y \in \mathbb{C} \), exactly one of the following is true: \( x \ll y \), \( y \ll x \), or \( x = y \)). First for transitivity, let \( x, y, z \in \mathbb{C} \), \( x = a + bi \), \( y = c + di \), \( z = e + fi \) such that \( x \ll y \ll z \). Therefore \( a \leq c \leq e \), so \( a \leq e \) by the transitivity of the order on \( \mathbb{R} \). If \( a < e \), then \( x \ll z \), so we are done. If \( a = e \), then \( a = c = e \) so we have from the definition of \( \ll \) that \( b < d < f \), so once again by the transitivity of the order on \( \mathbb{R} \), \( b < f \). Now \( a = e \) and \( b < f \Rightarrow x \ll z \), so we have shown transitivity.

Now to show totality. Consider \( x, y \in \mathbb{C} \), \( x = a + bi \), \( y = c + di \). Without loss of generality, let \( a \leq c \). Suppose \( a = c \). Then \( b < d \Leftrightarrow x \ll y \), \( b > d \Leftrightarrow y \ll x \), and \( b = d \Leftrightarrow x = y \), so by the totality of the order on \( \mathbb{R} \), we have the totality of \( \ll \) on \( \mathbb{C} \) in the case of \( a = c \). Suppose instead that \( a < c \). Then we know \( x \ll y \), and it is not the case that \( y \ll x \) or \( x = y \), so we have totality in this case as well. Thus we have proven that \( \ll \) is an order on \( \mathbb{C} \).

This order does not have the least-upper-bound property. Consider the set of complex numbers with real part less than or equal to zero:
\[ S = \{ a + bi : a \leq 0, b \in \mathbb{R} \}. \]

\( S \) is bounded above, for instance by the number 1, but it is not possible for any number \( z = a + bi \) to be the supremum of \( S \). If \( a \leq 0 \), then \( a + bi \ll a + (b + 1)i \in S \), so \( a + bi \) is not an upper bound for \( S \). If \( a > 0 \), then \( a + (b - 1)i \ll a + bi \), and \( a + (b - 1)i \) is also an upper bound for \( S \), so \( a + bi \) is not the least upper bound. Therefore \( S \) has no least upper bound, even though it is bounded above.

7) \( x, y \in \mathbb{R}^k \), so let \( x = (a_1, a_2, \ldots, a_k) \), \( y = (b_1, b_2, \ldots, b_k) \). Then
\[
|x + y|^2 + |x - y|^2 = \sum_{i=1}^{k} (a_i + b_i)^2 + \sum_{j=1}^{k} (a_j - b_j)^2 = \sum_{i=1}^{k} (a_i + b_i)^2 + (a_i - b_i)^2
\]
\[= \sum_{i=1}^{k} (a_i^2 + 2a_i b_i + b_i^2 + a_i^2 - 2a_i b_i + b_i^2) = \sum_{i=1}^{k} (2a_i^2 + 2b_i^2) = 2(|x|)^2 + 2(|y|)^2. \]

The geometric interpretation comes from looking at the parallelogram whose vertices are the points 0, \( x \), \( x + y \) and \( y \). Then the equation states that the sum of the squares of the lengths of the two diagonals (the vectors \( x + y \) and \( x - y \)) is the same as the sum of the squares of the lengths of the four sides.

\(^2\)A different proof of \( b^{r+s} \leq b^r b^s \) could start by justifying \( b^r = \inf\{b^r : r \in \mathbb{Q}, r \geq z \} \) and then proceeding as in the proof of \( b^r b^y \leq b^{r+y} \).