MATH 413 [513] (PHILLIPS) SOLUTIONS TO HOMEWORK 1

Generally, a "solution" is something that would be acceptable if turned in in the form presented here, although the solutions given are often close to minimal in this respect. A "solution (sketch)" is too sketchy to be considered a complete solution if turned in; varying amounts of detail would need to be filled in.

Problem 1.1: If $r \in \mathbb{Q} \setminus \{0\}$ and $x \in \mathbb{R} \setminus \mathbb{Q}$, prove that $r + x \notin \mathbb{Q}$ and $rx \notin \mathbb{Q}$.

Solution. We prove this by contradiction. Let $r \in \mathbb{Q} \setminus \{0\}$, and suppose that $r+x \in \mathbb{Q}$. Then, using the field properties of both $\mathbb{R}$ and $\mathbb{Q}$, we have $x = (r + x) - r \in \mathbb{Q}$. Thus $x \notin \mathbb{Q}$ implies $r + x \notin \mathbb{Q}$.

Similarly, if $rx \in \mathbb{Q}$, then $x = (rx)/r \in \mathbb{Q}$. (Here, in addition to the field properties of $\mathbb{R}$ and $\mathbb{Q}$, we use $r \neq 0$.) Thus $x \notin \mathbb{Q}$ implies $rx \notin \mathbb{Q}$. □

Problem 1.2: Prove that there is no $x \in \mathbb{Q}$ such that $x^2 = 12$.

Solution. We prove this by contradiction. Suppose there is $x \in \mathbb{Q}$ such that $x^2 = 12$. Write $x = \frac{m}{n}$ in lowest terms. Then $x^2 = 12$ implies $m^2 = 12n^2$. Since 3 divides $12n^2$, it follows that 3 divides m^2. Since 3 is prime (and by unique factorization in $\mathbb{Z}$), it follows that 3 divides m. Therefore 3^2 divides $m^2 = 12n^2$. Since 3^2 does not divide 12, using again unique factorization in $\mathbb{Z}$ and the fact that 3 is prime, it follows that 3 divides n. We have proved that 3 divides both m and n, contradicting the assumption that the fraction $\frac{m}{n}$ is in lowest terms. □

Alternate solution (sketch). If $x \in \mathbb{Q}$ satisfies $x^2 = 12$, then $\frac{x}{2}$ is in $\mathbb{Q}$ and satisfies $\left(\frac{x}{2}\right)^2 = 3$. Now prove that there is no $y \in \mathbb{Q}$ such that $y^2 = 3$ by repeating the proof that $\sqrt{2} \notin \mathbb{Q}$. □

One can avoid using unique factorization as follows, although one is using something else from elementary number theory (a particular case of the Euclidean Algorithm). For example, we need to show that if $m \in \mathbb{Z}$ and 3 divides m^2, then 3 divides m. Suppose that 3 does not divide m. Then there is $k \in \mathbb{Z}$ such that $m = 3k + 1$, or there is $k \in \mathbb{Z}$ such that $m = 3k + 2$. In the first case, $m^2 = 3(3k^2 + 2k) + 1$, which is not divisible by 3, and in the second case, $m^2 = 3(3k^2 + 6k + 1) + 1$, which is not divisible by 3.

Problem 1.5: Let $A \subset \mathbb{R}$ be nonempty and bounded below. Set $-A = \{-a \colon a \in A\}$. Prove that $\inf(A) = -\sup(-A)$.

Solution. We claim that that $-A$ is nonempty and bounded above. Indeed, there is some element $x \in A$, and then $-x \in A$; moreover, A has a lower bound m, and $-m$ is then an upper bound for $-A$. The claim is proved.

We now know that $b = \sup(-A)$ exists. We claim that $-b = \inf(A)$. That $-b$ is a lower bound for A is immediate from the fact that b is an upper bound for $-A$. To show that $-b$ is the greatest lower bound, we let $c > -b$ and prove that c is

Date: 1 October 2018.

not a lower bound for A. Now $-c < b$, so $-c$ is not an upper bound for $-A$. Thus there exists $x \in -A$ such that $x > -c$. Then $-x \in A$ and $-x < c$. So c is not a lower bound for A. The claim is proved. □

Problem 1.6: Let $b \in \mathbb{R}$ with $b > 1$, fixed throughout the problem.

As stated in the assignment, we will assume known that the function $n \mapsto b^n$, from $\mathbb{Z}$ to $\mathbb{R}$, is strictly increasing, that is, that for m, $n \in \mathbb{Z}$, we have $b^m < b^n$ if and only if $m < n$. Similarly, we take as known that $x \mapsto x^n$ is strictly increasing on $[0, \infty)$ when n is an *integer* with $n > 0$. We will also assume that the usual laws of exponents are known to hold when the exponents are *integers*. We can't assume anything about fractional exponents, except for Theorem 1.21 of the book and its corollary, because the context makes it clear that we are to assume fractional powers have not yet been defined.

(a) Let m, n, p, $q \in \mathbb{Z}$, with $n > 0$ and $q > 0$. Prove that if $\frac{m}{n} = \frac{p}{q}$, then $(b^m)^{1/n} = (b^p)^{1/q}$.

Solution. By the uniqueness part of Theorem 1.21 of the book, applied to the positive integer nq, it suffices to show that

$$\left[(b^m)^{1/n}\right]^{nq} = \left[(b^p)^{1/q}\right]^{nq}.$$

Now the definition in Theorem 1.21 implies that

$$\left[(b^m)^{1/n}\right]^{n} = b^m \qquad \text{and} \qquad \left[(b^p)^{1/q}\right]^{q} = b^p.$$

Therefore, using the laws of integer exponents and the equation $mq = np$, we get

$$\begin{aligned}\left[(b^m)^{1/n}\right]^{nq} &= \left[\left[(b^m)^{1/n}\right]^{n}\right]^{q} = (b^m)^q = b^{mq} \\ &= b^{np} = (b^p)^n = \left[\left[(b^p)^{1/q}\right]^{q}\right]^{n} = \left[(b^p)^{1/q}\right]^{nq},\end{aligned}$$

as desired. □

By Part (a), it makes sense to define $b^{m/n} = (b^m)^{1/n}$ for m, $n \in \mathbb{Z}$ with $n > 0$. This defines b^r for all $r \in \mathbb{Q}$.

(b) Prove that $b^{r+s} = b^r b^s$ for r, $s \in \mathbb{Q}$.

Solution. Choose m, n, p, $q \in \mathbb{Z}$, with $n > 0$ and $q > 0$, such that $r = \frac{m}{n}$ and $s = \frac{p}{q}$. Then $r + s = \frac{mq+np}{nq}$. By the uniqueness part of Theorem 1.21 of the book, applied to the positive integer nq, it suffices to show that

$$\left[b^{(mq+np)/(nq)}\right]^{nq} = \left[(b^m)^{1/n}(b^p)^{1/q}\right]^{nq}. \tag{1}$$

Directly from the definitions, we can write

$$\left[b^{(mq+np)/(nq)}\right]^{nq} = \left[\left[b^{(mq+np)}\right]^{1/(nq)}\right]^{nq} = b^{(mq+np)}.$$

Using the laws of integer exponents and the definitions for rational exponents, we can rewrite the right hand side of (1) as

$$\left[(b^m)^{1/n}(b^p)^{1/q}\right]^{nq} = \left[\left[(b^m)^{1/n}\right]^{n}\right]^{q}\left[\left[(b^p)^{1/q}\right]^{q}\right]^{n} = (b^m)^q(b^p)^n = b^{(mq+np)}.$$

This proves the required equation, and hence the result. □

(c) For $x \in \mathbb{R}$, define

$$B(x) = \{b^r : r \in \mathbb{Q} \cap (-\infty, x]\}.$$

Prove that if $r \in \mathbb{Q}$, then $b^r = \sup(B(r))$.

Solution. We claim that if r, $s \in \mathbb{Q}$ with $r < s$, then $b^r < b^s$. (This is the main point.) To prove the claim, choose m, n, p, $q \in \mathbb{Z}$, with $n > 0$ and $q > 0$, such that $r = \frac{m}{n}$ and $s = \frac{p}{q}$. Then also $r = \frac{mq}{nq}$ and $s = \frac{np}{nq}$, with $nq > 0$, so

$$b^r = (b^{mq})^{1/(nq)} \qquad \text{and} \qquad b^s = (b^{np})^{1/(nq)}.$$

Now $mq < np$ because $r < s$. Therefore, using the definition of $c^{1/(nq)}$,

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

Since $x \mapsto x^{nq}$ is strictly increasing, this implies that $b^r < b^s$. The claim is proved.

Now we can prove that if $r \in \mathbb{Q}$ then $b^r = \sup(B(r))$. By the claim, if $s \in \mathbb{Q}$ and $s \leq r$, then $b^s \leq b^r$. This implies that b^r is an upper bound for $B(r)$. Since $b^r \in B(r)$, obviously no number smaller than b^r can be an upper bound for $B(r)$. So $b^r = \sup(B(r))$. □

We now define $b^x = \sup(B(x))$ for every $x \in \mathbb{R}$. We need to show that $B(x)$ is nonempty and bounded above. To show it is nonempty, choose (using the Archimedean property) some $k \in \mathbb{Z}$ with $k < x$; then $b^k \in B(x)$. To show it is bounded above, similarly choose some $k \in \mathbb{Z}$ with $k > x$. If $r \in \mathbb{Q} \cap (-\infty, x]$, then $b^r \in B(k)$ so that $b^r \leq b^k$ by Part (c). Thus b^k is an upper bound for $B(x)$. This shows that the definition makes sense, and Part (c) shows it is consistent with our earlier definition when $r \in \mathbb{Q}$.

(d) Prove that $b^{x+y} = b^x b^y$ for all x, $y \in \mathbb{R}$.

In order to do this, we are going to need to replace the set $B(x)$ above by the set

$$B_0(x) = \{b^r : r \in \mathbb{Q} \cap (-\infty, x)\}$$

(that is, we require $r < x$ rather than $r \leq x$) in the definition of b^x. (If you are skeptical, read the main part of the solution first to see how this is used.)

We show that the replacement is possible via some lemmas.

Lemma 1. If $x \in [0, \infty)$ and $n \in \mathbb{Z}_{\geq 0}$, then $(1 + x)^n \geq 1 + nx$.

Proof. The proof is by induction on n. The statement is obvious for $n = 0$. So assume it holds for some $n \in \mathbb{Z}_{\geq 0}$. Then, using the induction hypothesis and $1 + x \geq 0$ at the second step,

$$\begin{aligned}(1 + x)^{n+1} &= (1 + x)^n (1 + x) \geq (1 + nx)(1 + x) \\ &= 1 + (n + 1)x + nx^2 \geq 1 + (n + 1)x.\end{aligned}$$

This proves the result for $n + 1$. □

Lemma 2. We have $\inf\big(\{b^{1/n} : n \in \mathbb{Z}_{>0}\}\big) = 1$.

Recall that $b > 1$.

Proof of Lemma 2. Clearly 1 is a lower bound. (Indeed, $(b^{1/n})^n = b > 1 = 1^n$, so $b^{1/n} > 1$.) We finish the proof by showing that if $x > 0$ then $1 + x$ is not a lower bound. If $1 + x$ were a lower bound, then $1 + x \leq b^{1/n}$ would imply $(1 + x)^n \leq (b^{1/n})^n = b$ for all $n \in \mathbb{Z}_{>0}$. By Lemma 1, we would get $1 + nx \leq b$ for all $n \in \mathbb{Z}_{>0}$, which contradicts the Archimedean property when $x > 0$. □

Lemma 3. We have $\sup\big(\{b^{-1/n} \colon n \in \mathbb{Z}_{>0}\}\big) = 1$.

Proof. Part (b) shows that $b^{-1/n}b^{1/n} = b^0 = 1$, whence $b^{-1/n} = (b^{1/n})^{-1}$. Since all numbers $b^{-1/n}$ are strictly positive, it now follows from Lemma 2 that 1 is an upper bound. Suppose $x < 1$ is an upper bound. Then x^{-1} is a lower bound for $\{b^{1/n} \colon n \in \mathbb{Z}_{>0}\}$. Since $x^{-1} > 1$, this contradicts Lemma 2. Thus $\sup\{b^{-1/n} \colon n \in \mathbb{Z}_{>0}\} = 1$, as claimed. □

Lemma 4. If $x \in \mathbb{R}$ then $b^x = \sup(B_0(x))$.

Proof. If $x \notin \mathbb{Q}$, then $B_0(x) = B(x)$, so there is nothing to prove. If $x \in \mathbb{Q}$, then at least $B_0(x) \subset B(x)$, so $b^x \geq \sup(B_0(x))$. Moreover, Part (b) shows that $b^{x-1/n} = b^x b^{-1/n}$ for $n \in \mathbb{Z}_{>0}$. The numbers $b^{x-1/n}$ are all in $B_0(x)$, and

$$\sup\{b^x b^{-1/n} \colon n \in \mathbb{Z}_{>0}\} = b^x \sup\{b^{-1/n} \colon n \in \mathbb{Z}_{>0}\}$$

because $b^x > 0$, so using Lemma 3 in the last step gives

$$\sup(B_0(x)) \geq \sup\{b^{x-1/n} \colon n \in \mathbb{Z}_{>0}\} = b^x \sup\{b^{-1/n} \colon n \in \mathbb{Z}_{>0}\} = b^x.$$

This completes the proof. □

Now we can prove the formula $b^{x+y} = b^x b^y$.

Solution. We first show that $b^{x+y} \leq b^x b^y$, which we do by showing that $b^x b^y$ is an upper bound for $B_0(x + y)$. Thus let $r \in \mathbb{Q}$ satisfy $r < x + y$. Then there are s_0, $t_0 \in \mathbb{R}$ such that $r = s_0 + t_0$ and $s_0 < x$, $t_0 < y$. Choose s, $t \in \mathbb{Q}$ such that $s_0 < s < x$ and $t_0 < t < y$. Then $r < s + t$, so $b^r < b^{s+t} = b^s b^t \leq b^x b^y$. This shows that $b^x b^y$ is an upper bound for $B_0(x + y)$, proving the claim.

(Note that this does not work using $B(x + y)$. If $x + y \in \mathbb{Q}$ but x, $y \notin \mathbb{Q}$, then $b^{x+y} \in B(x + y)$, but it is not possible to find s and t with $b^s \in B(x)$, $b^t \in B(y)$, and $b^s b^t = b^{x+y}$.)

We now prove the reverse inequality. Suppose it fails, that is, $b^{x+y} < b^x b^y$. Then

$$\frac{b^{x+y}}{b^y} < b^x.$$

The left hand side is thus not an upper bound for $B_0(x)$, so there exists $s \in \mathbb{Q}$ with $s < x$ and

$$\frac{b^{x+y}}{b^y} < b^s.$$

It follows that

$$\frac{b^{x+y}}{b^s} < b^y.$$

Repeating the argument, there is $t \in \mathbb{Q}$ with $t < y$ such that

$$\frac{b^{x+y}}{b^s} < b^t.$$

Therefore, by Part (b),

$$b^{x+y} < b^s b^t = b^{s+t}.$$

But $b^{s+t} \in B_0(x+y)$ because $s+t \in \mathbb{Q}$ and $s+t < x+y$, so this is a contradiction. Therefore $b^{x+y} \leq b^x b^y$. □

Problem 1.9: Define a relation on $\mathbb{C}$ by $w < z$ if and only if either $\mathrm{Re}(w) < \mathrm{Re}(z)$ or both $\mathrm{Re}(w) = \mathrm{Re}(z)$ and $\mathrm{Im}(w) < \mathrm{Im}(z)$. (For $z \in \mathbb{C}$, the expressions $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ denote the real and imaginary parts of z.) Prove that this makes $\mathbb{C}$ an ordered set. Does this order have the least upper bound property?

Solution. We verify the two conditions in the definition of an order. For the first, let w, $z \in \mathbb{C}$. There are three cases.

Case 1: $\mathrm{Re}(w) < \mathrm{Re}(z)$. Then $w < z$, but $w = z$ and $w > z$ are both false.

Case 2: $\mathrm{Re}(w) > \mathrm{Re}(z)$. Then $w > z$, but $w = z$ and $w < z$ are both false.

Case 3: $\mathrm{Re}(w) = \mathrm{Re}(z)$. This case has three subcases.

Case 3.1: $\mathrm{Im}(w) < \mathrm{Im}(z)$. Then $w < z$, but $w = z$ and $w > z$ are both false.

Case 3.2: $\mathrm{Im}(w) > \mathrm{Im}(z)$. Then $w > z$, but $w = z$ and $w < z$ are both false.

Case 3.3: $\mathrm{Im}(w) = \mathrm{Im}(z)$. Then $w = z$, but $w > z$ and $w < z$ are both false.

These cases exhaust all possibilities, and in each of them exactly one of $w < z$, $w = z$, and $w > z$ is true, as desired.

Now we prove transitivity. Let $s < w$ and $w < z$. If either $\mathrm{Re}(s) < \mathrm{Re}(w)$ or $\mathrm{Re}(w) < \mathrm{Re}(z)$, then clearly $\mathrm{Re}(s) < \mathrm{Re}(z)$, so $s < z$. If $\mathrm{Re}(s) = \mathrm{Re}(w)$ and $\mathrm{Re}(w) = \mathrm{Re}(z)$, then the definition of the order requires $\mathrm{Im}(s) < \mathrm{Im}(w)$ and $\mathrm{Im}(w) < \mathrm{Im}(z)$. We thus have $\mathrm{Re}(s) = \mathrm{Re}(z)$ and $\mathrm{Im}(s) < \mathrm{Im}(z)$, so $s < z$ by definition.

It remains to answer the last question. We show that this order does not have the least upper bound property. Let $S = \{z \in \mathbb{C} \colon \mathrm{Re}(z) < 0\}$. Then $S \neq \varnothing$ because $-1 \in S$, and S is bounded above because 1 is an upper bound for S.

We show that S does not have a least upper bound by showing that if w is an upper bound for S, then there is a smaller upper bound. First, by the definition of the order it is clear that $\mathrm{Re}(w)$ is an upper bound for

$$\{\mathrm{Re}(z) \colon z \in S\} = (-\infty, 0).$$

Therefore $\mathrm{Re}(w) \geq 0$. Moreover, every $u \in \mathbb{C}$ with $\mathrm{Re}(u) \geq 0$ is in fact an upper bound for S. In particular, if w is an upper bound for S, then $w - i < w$ and has the same real part, so is a smaller upper bound. □

Note: A related argument shows that the set $T = \{z \in \mathbb{C} \colon \mathrm{Re}(z) \leq 0\}$ also has no least upper bound. One shows that w is an upper bound for T if and only if $\mathrm{Re}(w) > 0$.

Problem 1.13: Prove that if x, $y \in \mathbb{C}$, then $\big||x| - |y|\big| \leq |x - y|$.

Solution. The desired inequality is equivalent to

$$|x| - |y| \leq |x - y| \qquad \text{and} \qquad |y| - |x| \leq |x - y|.$$

We prove the first; the second follows by exchanging x and y.

Set $z = x - y$. Then $x = y + z$. The triangle inequality gives $|x| \leq |y| + |z|$. Substituting the definition of z and subtracting $|y|$ from both sides gives the result. □

Problem 1.17: Prove that if x, $y \in \mathbb{R}^n$, then

$$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2.$$

Interpret this result geometrically in terms of parallelograms.

Solution. Using the definition of the norm in terms of scalar products, we have:

$$\begin{aligned}\|x+y\|^2 + \|x-y\|^2 &= \langle x+y, x+y\rangle + \langle x-y, x-y\rangle \\ &= \langle x,x\rangle + \langle x,y\rangle + \langle y,x\rangle + \langle y,y\rangle \\ &\qquad + \langle x,x\rangle - \langle x,y\rangle - \langle y,x\rangle + \langle y,y\rangle \\ &= 2\langle x,x\rangle + 2\langle y,y\rangle = 2\|x\|^2 + 2\|y\|^2,\end{aligned}$$

as desired.

The interpretation is that 0, x, y, and $x+y$ are the vertices of a parallelogram, and that $\|x+y\|$ and $\|x-y\|$ are the lengths of its diagonals while $\|x\|$ and $\|y\|$ are each the lengths of two opposite sides. Therefore the sum of the squares of the lengths of the diagonals is equal to the sum of the squares of the lengths of the sides. □

One can do the proof directly in terms of the formula $\|x\|^2 = \sum_{k=1}^n |x_k|^2$. The steps are all the same, but it is more complicated to write. It is also less general, since the argument above applies to any norm that comes from a scalar product.