Math 571 - Homework 1 (Due 5/17/23)

Problem 0.1 (R:1:2*)**.** Show that for any positive integer n, if n is not a perfect square, then $\sqrt{n}$ is irrational.

Suppose $\sqrt{n} = p/q$ where p and q are integers with no common factors, i.e., $\gcd(p, q) = 1$. Then $n = p^2/q^2$ so $nq^2 = p^2$. But we know that $\gcd(p^2, q^2) = 1$ and that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$, thus $p^2|n$. This means $n = n'p^2$ and so $n'q^2 = 1$, thus $n' = 1$ hence $n = p^2$.

Problem 0.2 (R:1:4*)**.** Let E be a non-empty subset of an ordered set $(S, <)$; suppose that α is a lower bound for E in S and β is an upper-bound for E in S. Show that $\alpha \leq \beta$. Can $\alpha = \beta$? Is this still true if $E = \emptyset$?

As E is non-empty, let $s \in E$, then $\alpha \leq s \leq \beta$. It could be that $E = \{s\}$ and so $\alpha = s = \beta$. If $E = \emptyset$, then for $s \in S$, s is both a lower-bound and an upper-bound for E, thus if $|S| > 1$ it is possible that $\beta < \alpha$.

Problem 0.3 (R:1:5)**.** Let A be a non-empty set of real numbers bounded below. Let $-A = \{-a \mid a \in A\}$. Show that

$$\inf(A) = -\sup(-A)$$

Let $\alpha = \inf(A)$. We have $\alpha \leq a$ for all $a \in A$ and thus $-\alpha \geq -a$ for all $a \in A$. So $-A$ is bounded above by $-\alpha$.

Suppose that β is any upper-bound for $-A$, then, as above, $-\beta$ is a lower-bound for A and hence $-\beta \leq \alpha$, but then $-\alpha \leq \beta$. Thus $-\alpha = \sup(-A)$. This yields the desired result.

Problem 0.4 (R:1:6)**.** Fix $b > 1$.

(a) If n, m, p, q are integers, $n, q > 0$, and $r = m/n = p/q$, prove that

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

Explain why it makes sense to define $b^r = (b^m)^{1/n}$.

The equality is trivial

$$(b^m)^{1/n} = (b^p)^{1/q} \iff ((b^m)^{1/n})^{nq} = ((b^p)^{1/q})^{nq} \iff b^{mq} = b^{pn} \iff mq = pn$$

Because of this it makes sense to define $b^r = b^{m/n}$ where $r = m/n$ for any m, n such that $r = m/n$.

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

Let $r = m/n$ and $s = p/q$, then

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

Here we do use that $x^{1/k}y^{1/k} = (xy)^{1/k}$ this is easily shown by

$$\begin{aligned} x^{1/k} = a \text{ and } y^{1/k} = b &\iff x = a^k \text{ and } b = y^k && (1)\\ &\implies xy = a^k b^k = (ab)^k && (2)\\ &\iff (xy)^{1/k} = ab = x^{1/k}y^{1/k} && (3) \end{aligned}$$

(c) If $x \in \mathbb{R}$, define $B(x) = \{b^t \mid t \in \mathbb{Q} \wedge t \leq x\}$. Prove that

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

when r is rational. Explain why it makes sense to define

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

for every real x.

Suppose $r < s$ are rational, then $b^{s-r} = b^{m/n}$ where $m/n > 0$. Clearly, $b^m > 1$ and if $a^n = b^m$, then $a > 1$ so $b^{m/n} = b^{s-r} > 1$, that means $b^s/b^r > 1$ and so $b^s > b^r$.

This implies immediately that $b^r = \sup(B(r))$.

We know $B(x)$ is bounded above for each $x \in \mathbb{R}$ since if $r \in \mathbb{Q}$ and $r > x$ we have $b^r \geq B(x)$. So $b^x = \sup(B(x))$ exists.

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

Let's see that $B(x)B(y) = B(x+y)$. Suppose $b^r = b^s b^t \in B(x)B(y)$, then $s \leq x$ and $t \leq y$ so $r = s + t \leq x + y$ and $b^r = b^{s+t} \in B(x+y)$. Conversely, take $b^r \in B(x+y)$, then $r < x + y$. Then $r - y < x$ and we get $r - y < t < x$. But $s = r - t < y$ so $r = s + t$ with $r < x$ and $s < y$, hence $b^r = b^s b^t \in B(x)B(y)$. So $b^{x+y} = \sup(B(x)B(y))$.

We need to see that $\sup(B(x)B(y)) = \sup(B(x))\sup(B(y))$. Clearly, $b^x b^y = \sup(B(x))\sup(B(y)) \geq B(x)B(y)$ so $b^x b^y \geq \sup(B(x)B(y)) = \sup(B(x+y)) = b^{x+y}$.

To finish, show $\sup(B(x+y)) \leq \sup(B(x))\sup(B(y))$. Suppose $a < b^x b^y$, then $a/b^x < b^y$ so there is $r < y$ with $a/b^x < b^r$. Now $a/b^r < b^x$ so there is $s < x$ with $a/b^r < b^s$ so $a < b^r b^s < \sup(B(x)B(y))$ Thus $b^x b^y \leq \sup(B(x)B(y))$.

Problem 0.5 (R:1:8)**.** Show that $\mathbb{C}$ can not be made into an ordered field.

This is "sort of" trivial. In an ordered field, $a^2 \geq 0$ for all a. This is by definition for $a > 0$ and trivial for $a = 0$ so we need to see that it holds for $a < 0$. If $a < 0$, then $-a > 0$, this is because $a > 0 \implies 0 = a + (-a) > 0 + (-a) = -a$. So $(-a)(-a) > 0$, if we can just show $(-a)(-a) = a^2$, then we are done.

For this it would be nice to argue $(-a) = -1(a)$ and so $(-a)(-a) = (-1)^2a^2$ and then we just need to see that $(-1)^2 = 1^2$. If we knew $0a = 0$, then $(1 + (-1))a = 0$ so $1a + (-1)a = a + (-1)a = 0$ and by the uniqueness of inverses, $(-1)a = -a$. This also gives $(-1)^2 = -1(-1) = -(-1) = 1$.

So we need $0a = 0$ and we are done. For this we have $0a + a = 1a + 1a = (0 + 1)a = 1a = a$. So $0a + a = a$. adding $-a$ to both sides gives $0a = 0$. Yeah!

Problem 0.6 (R:1:14*)**.** Show that for $w, z \in \mathbb{C}$

$$|w + z|^2 + |w - z|^2 = 2|w|^2 + 2|z|^2.$$

Use this to compute $|1 + z|^2 + |1 - z|^2$ given that $|z| = 1$.

Getting $|1 + z|^2 + |1 - z|^2 = 2|w| + 2|z| = 2 + 2 = 4$ given that $|z| = 1$ is trivial by letting $w = 1$.

For the main part we have

$$\begin{aligned}
|w + z|^2 + |w - z|^2 &= (w + z)\overline{(w + z)} + (w - z)\overline{(w - z)} \\
&= (w + z)(\bar{w} + \bar{z}) + (w - z)(\bar{w} - \bar{z}) \\
&= w\bar{w} + z\bar{w} + w\bar{z} + z\bar{z} + w\bar{w} - z\bar{w} - w\bar{z} + z\bar{z} \\
&= 2|w|^2 + 2|z|^2
\end{aligned}$$

Problem 0.7 (R:1:17)**.** Show that for $x, y \in \mathbb{R}^k$,

$$\|x + y\|_2^2 + \|x - y\|_2^2 = 2\|x\|_2^2 + 2\|y\|_2^2. \tag{Parallelogram Law}$$

How does this generalize the Pythagorean theorem?

This is proved exactly as in the previous problem:

$$\begin{aligned}
\|x + y\|_2^2 + \|x - y\|_2^2 &= (x + y)^H(x + y) + (x - y)^H(x - y) \\
&= (x^H + y^H)(x + y) + (x^H - y^h)(x - y) \\
&= x^Hx + x^Hy + y^Hx + y^Hy + x^Hx - x^Hy - y^Hx + y^H)y \\
&= 2\|x\|_2^2 + 2\|y\|_2^2
\end{aligned}$$

Problem 0.8 (R:1:18)**.** Show that if $k \geq 2$ and $x \in \mathbb{R}^k$, there is $y \in \mathbb{R}^k$, $y \neq 0$ such that $\langle x, y\rangle = 0$.

If you recall how this goes, drop the $k \geq 2$ and show that given any non-zero pairwise orthogonal $x_1, x_2, \ldots, x_l$ $(l \leq k)$ in $\mathbb{R}^k$, you can find $x_{l+1}, \ldots, x_k$ so that $x_1, x_2, \ldots, x_k$ are pairwise orthogonal.

This is basically Gram-Schmidt from linear algebra. For just one vector x, take y such that $y \neq \alpha x$, then set $\hat{y} = y - \frac{\langle x,y\rangle}{\langle x,x\rangle}x$. Note that

$$\langle x, \hat{y}\rangle = \left\langle x, y - \frac{\langle x, y\rangle}{\langle x, x\rangle}x \right\rangle = \langle x, y\rangle - \frac{\langle x, y\rangle}{\langle x, x\rangle}\langle x, x\rangle = \langle x, y\rangle - \langle x, y\rangle = 0$$

Notice that if x were a unit vector, then the orthogonal projection of y onto x is just $\langle x, y\rangle x$ and so $\hat{y} = \langle x, y\rangle x$.

If $\{x_1, \ldots, x_k\}$ are mutually orthogonal unit vectors, then the orthogonal projection of y onto $S = \text{span}\{x_1, \ldots, x_k\}$ is

$$\text{proj}_S^{\perp}(y) = \sum_{i=1}^{k} \langle y, x_i\rangle x_i$$

From the Pythagorean theorem, this is the point in S *closest* to y in the $\|\cdot\|_2$-norm.