# Math 571 - Homework 1

**Problem 1.1** (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 $n' = 1$ and $q = 1$ hence $n = p^2$.

**Problem 1.2** (R:1:4*)**.** Let $E$ be a non-empty subset of an ordered set $(S, <)$; suppose that $\alpha$ is a lower bound for $E$ in $S$ and $\beta$ is an upper bound for $E$ in $S$. Show that $\alpha \leq \beta$. Can $\alpha = \beta$? What happens 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 1.3** (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 $\beta$ 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 1.4** (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

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

Because of this defining $b^r$ and $b^{m/n}$ for any $m/n = r$ provided $n > 0$ is well-defined.

With $a, b, c > 0$ real and $i, k, n, q > 0$ and $m, p$ all integers. Equality can be argued as follows:

$$\begin{aligned}
(b^m)^{1/n} = (b^p)^{1/q} &\iff ((b^m)^{1/n})^{nq} = ((b^p)^{1/q})^{nq} && \text{since } a^i = c^i \iff a = c \\
&\iff b^{mq} = b^{pn} && \text{since } (a^{1/i})^i = a \\
&\iff mq = pn && \text{since } a^i = a^k \iff i = k
\end{aligned}$$

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

$$\begin{aligned} b^{r+s} &= b^{(qm+np)/qn} && \text{since } r+s = (qm+np)/qn \\ &= (b^{qm+np})^{1/nq} && \text{by (a)} \\ &= (b^{qm}b^{np})^{1/nq} \\ &= (b^{qm})^{1/nq}(b^{np})^{1/nq} && \text{since } (ac)^{1/k} = a^{1/k}c^{1/k} \\ &= b^r b^s && \text{by (a)} \end{aligned}$$

Here we do use that $a^{1/k}c^{1/k} = (ac)^{1/k}$ this is easily shown by

$$\begin{aligned} a^{1/k} = \alpha \text{ and } c^{1/k} = \gamma &\iff a = \alpha^k \text{ and } c = \gamma^k \\ &\implies ac = \alpha^k\gamma^k = (\alpha\gamma)^k \\ &\iff (ac)^{1/k} = \alpha\gamma = a^{1/k}c^{1/k} \end{aligned}$$

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

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

whenever $r$ is rational.

Explain why it makes sense to define

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

for every real $x$.

Suppose $m/n = r < s = p/q$ are rational with $n, q > 0$, then $mq < np$ and

$$b^{mq} < b^{np} \iff b^{mq/nq} < b^{np/nq} \iff b^r < b^s$$

So $b^r \geq B(r)$. Since, in addition, $b^r \in B(r)$ we have 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. We have also seen that defining $b^x$ in this manner extends the map $r \mapsto b^r$ for $r \in \mathbb{Q}$. Later, we will see that this is the *unique* continuous extension to $\mathbb{R}$ of this map.

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

We need to see that

$$\sup(B(x))\sup(B(y)) = \sup(B(x+y))$$

First argue that $\sup(B(x+y)) \leq \sup(B(x))\sup(B(y))$:

Suppose one of $x$ or $y$ is not rational. For specificity, suppose it is $y$. Then $B(y) = \{b^t \mid t < y\}$ and so we know that for all $t < y$, there is $t < t' < y$ with $b^{t'} \in B(y)$.

Suppose $\sup(B(x))\sup(B(y)) < \sup(B(x+y))$. Then $\sup(B(x)) < b^t/\sup(B(y))$ for some $t < x+y$. But then for all $s < x$, $b^s < b^t/\sup(B(y))$, consider, $b^{t-s} > \sup(B(y))$ for all $s < x$. But $t-s < y$ so choose $t' < y$. Then $b^{t-s} < b^{t'} \in B(y)$. This is a contradiction.

The other case is $x$ and $y$ are rational, and in this case, we already know $b^{x+y} = b^x b^y$ from the preceding part.

Next argue that $\sup(B(x))\sup(B(y)) \leq \sup(B(x+y))$:

Let $z < \sup(B(x))\sup(B(y))$, it suffices to see that $z < \sup(B(x+y))$. Since $z < \sup(B(x))\sup(B(y))$, $z/\sup(B(x)) < b^s \in B(y)$ for some rational $s$. This, in turn, means that $z/b^s < b^t \in B(y)$ for some rational $t$. So $z < b^s b^t = b^{s+t} \in B(x+y)$ and so $z < \sup(B(x+y))$, which is what we were trying to show.

**Problem 1.5** (R:1:7)**.** Fix $b > 1$, $y > 1$, and show that there is a unique $x$ so that $b^x = y$. This defines $\log_b(y) = x$.

(a) For any positive integer $n$, $b^n - 1 \geq n(b-1)$.

This is easy to see as

$$\frac{b^n - 1}{b-1} = \sum_{i=0}^{n-1} b^i \geq \sum_{i=0}^{n-1} 1 = n$$

Recall

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

Let $c = b^{1/n}$, then by (a), since $c > 1$,

$$c^n - 1 \geq n(c-1), \text{ so } b - 1 \geq n(b^{1/n} - 1)$$

(c) If $t > 1$ and $n(t-1) > (b-1)$, then $b^{1/n} < t$.

From (b) we have $t^n - 1 \geq n(t-1) > b - 1$, so $t^n > b$ and thus $t > b^{1/n}$ since $b^x$ is monotonic increasing.

(d) If $w$ is such that $b^w < y$, then $b^{w+1/n} < y$ for large enough $n$. To see this, apply (c) to $t = y \cdot b^{-w}$.

Let $t = y \cdot b^{-w}$, note that $t > 1$ by assumption. Take $n$ large enough so that

$$n > \frac{b-1}{t-1} = \frac{b-1}{y \cdot b^{-w} - 1}$$

By (c). $b^{1/n} < y \cdot b^{-w}$ and thus, $y > b^w b^{1/n} = b^{w+1/n}$. This is what we wanted.

(e) If $b^w > y$, then $b^{w-1/n} > y$ for large enough $n$.

Imitate the above, let $t = y^{-1} \cdot b^w > 1$ and let $n$ be large enough so that $n > \frac{b-1}{t-1}$, then again by (c), $b^{1/n} < y^{-1} \cdot b^w$. Thus we get $y < b^w \cdot b^{-1/n} = b^{w-1/n}$.

(f) Let $A(y) = \{w \mid b^w < y\}$ and $x = \sup(A(y))$. Show that $y = b^x$.

Before starting this argument, notice that $A(y)$ is the *obvious* set to try to use here. The argument below indicates how (d) and (e) are natural. Thus, (a)–(c) can be seen as technical steps used to prove (d) and (e).

Clearly, $A(y)$ is bounded above so that $x$ exists. $y \leq b^x$ since otherwise, $b^x < y$ hence $b^x \in A(y)$. By (d) this can't happen as $b^{x+1/n} < y$ for large enough $n$, so $x + 1/n \in A(y)$ contradicting $x = \sup(A(y))$.

If $y < b^x$, then by (e) $b^{x-1/n} > y$ for large enough $n$. But $x - 1/n < \sup(A(y))$ and so $b^{x-1/n} < y$. Thus $b^x \leq y$.

We have shown $b^x \leq y \leq b^x$ and so $y = b^x$.

(g) Show that $x$ is unique.

If $b^x = b^z = y$, then $b^x b^{-z} = b^{x-z} = 1$. So, it suffices to see that $b^x = 1 \implies x = 0$. But we already know that if $x > 0$, then $b^x > 1$ and if $x < 0$, then $b^x < 1$. So $x = 0$ as needed.

**Problem 1.6** (R:1:8)**.** Show that $\mathbb{C}$ can not be made into an ordered field.

We show that 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 $\boxed{(-a)(-a) = a^2}$.

For this it would be nice to argue $\boxed{(-a) = -1(a)}$ so that $(-a)(-a) = (-1)^2 a^2$. Then we just need to see that $\boxed{(-1)^2 = 1}$. If we knew $\boxed{0a = 0}$, 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 just need $0a = 0$. For this, we have $0a + a = 0a + 1a = (0+1)a = 1a = a$. So $0a + a = a$. Adding $-a$ to both sides gives $0a = 0$. Yeah!

**Problem 1.7** (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 1.8** (R:1:17)**.** Show that for $x, y \in \mathbb{R}^k(\mathbb{C}^k)$,

$$\|x+y\|_2^2 + \|x-y\|_2^2 = 2\|x\|_2^2 + 2\|y\|_2^2. \qquad \text{(Parallelogram Law)}$$

How does this generalize the Pythagorean theorem?

This is proved exactly as in the previous problem. The operation corresponding to conjugate above is the *Hermitian* or *Conjugate Transpose* (See here). $A^H = (\bar{A})^T = \overline{A^T}$

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

**Problem 1.9** (R:1:18)**.** Show that if $k \geq 2$ and $x \in \mathbb{R}^k(\mathbb{C}^k)$, there is $y \in \mathbb{R}^k(\mathbb{C}^k)$, $y \neq 0$ such that $\langle x, y\rangle = 0$.

If $x = 0$, then any $y$ would suffice, so suppose $x \neq 0$. Take any $z$ not of the form $cx$ for some scalar $c \in \mathbb{R}(\mathbb{C})$

Let $y = z - \frac{\langle x,z\rangle}{\langle x,x\rangle}x$. Note that $y \neq 0$ since $z \neq \frac{\langle x,z\rangle}{\langle x,x\rangle}x$ by assumption. Then

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

So $y \neq 0$ and $y \perp x$ as desired.

**Note:** This is a standard linear algebra construction:

$$\text{proj}_x(z) = \frac{\langle x,z\rangle}{\langle x,x\rangle}x \text{ is the } \textit{orthogonal projection of } z \textit{ onto } x$$
$$y = z - \text{proj}_x(z) \text{ is } \textit{the component of } z \textit{ orthogonal to } x$$

Officially, the projection of $z$ onto $x$ is the point (vector) $p$ on the line $l : cx$ so that $\|p - z\| \leq \|q - z\|$ for any $q$ on $l$. Essentially, the Pythagorean Theorem gives that $p$ is any (the unique) point in $l$ so that $z - p \perp l$.

The preceding computation is essentially the proof that if we take $p = \text{proj}_x(z)$ on $l$, then $z - p \perp l$.