Math 351 DNHI 1

Mario L. Gutierrez Abed

(1) If r is a rational $(r \neq 0)$ and x is irrational, prove that $r + x$ and $r\,x$ are irrational.

<u>Proof:</u>
If r and $r + x$ were both rational, then $r + x - r = x$ would also be rational, so we have a contradiction. $(\Rightarrow\Leftarrow)$ ✓
Similarly, if both r and $r\,x$ were rational, then $\frac{r\,x}{r} = x$ must also be rational, which again contradicts the assumption that x is irrational. $(\Rightarrow\Leftarrow)$ ✓ $\blacksquare$

(2) Prove that there is no rational number whose square is 12.

<u>Proof:</u>
Assume there exists such a rational number $r = \frac{m}{n}$ such that $\left(\frac{m}{n}\right)^2 = 12$, where $\frac{m}{n}$ is in simplest terms. Then this implies that $m^2 = 12\,n^2 \Longrightarrow m = 2\sqrt{3}\;n \Longrightarrow$ m is even. Since $\frac{m}{n}$ is assumed to be in simplest terms, n must be odd.
Thus, let $m = 2\,s \Longrightarrow s^2 = 3\,n^2$. Since n is odd so is s, hence we let $n = 2\,k + 1$, $s = 2\,c + 1$.

$$
\begin{aligned}
\text{Then } s^2 &= (2\,c+1)^2 = 3\,(2\,k+1)^2 \\
&= 4\,c^2 + 4\,c + 1 = 3\,(4\,k^2 + 4\,k + 1) \\
&= 4\,c^2 + 4\,c + 1 = 12\,k^2 + 12\,k + 3 \\
&= 4\,c^2 + 4\,c - 12\,k^2 - 12\,k - 2 = 0
\end{aligned}
$$

$$
\begin{aligned}
\text{Thus we have } s^2 &= 4\,c^2 + 4\,c - 12\,k^2 - 12\,k = 2 \\
&= 4\,(c^2 + c - 3\,k^2 - 3\,k) = 2
\end{aligned}
$$

This is absurd, because 2 cannot be a multiple of 4. Hence, our assumption that r existed is erroneous, and we conclude that no rational number has square 12. $\blacksquare$

<u>(Alternate) Proof:</u>
Suppose $\left(\frac{m}{n}\right)^2 = 12$ and $\gcd(m,\ n) = 1$. Then $m^2 = 4\,(3\,n^2)$, implying that $3 \mid m^2$. Since 3 is prime, $3 \mid m$. In particular, $m = 3\,k$ for some integer k.
Thus $m^2 = 9\,k^2 = 4\,(3\,n^2)$ or, equivalently, $3\,k^2 = 4\,n^2$. Since $3 \mid 4\,n^2$ and $3 \nmid 4$, it follows that $3 \mid n^2$ and, therefore, $3 \mid n$.
Thus, it follows that $n = 3\,p$ for some $p \in \mathbb{Z}$. $(\Rightarrow\Leftarrow)$
This is a contradiction because $\gcd(m,\ n) = \gcd(3\,k,\ 3\,p) \geq 3 > 1$,
and we assumed initially that $\gcd(m,\ n) = 1$. $\blacksquare$

(3) Let E be a nonempty subset of an ordered set; suppose α is a lower bound and β is an upper bound of E. Prove that $\alpha \leq \beta$.

Proof:
The subset E is nonempty, so there exists $x \in E$. Then, by the definition of lower and upper bounds, it must be true that $\alpha \leq x \leq \beta$. But then since E is ordered, it follows that $\alpha < \beta$. Otherwise we would have $\alpha = x = \beta$, which contraditcs our assumption that α and β are a lower bound and an upper bound of E, respectively. ■

(4) Let A be a nonempty set of real numbers which is bounded below. Let $-A$ be the set of all numbers $-x$, where $x \in A$. Prove that $\inf A = -\sup(-A)$.

Proof:
We have that A is not empty and is bounded below. What's more, since A is a bounded subset of $\mathbb{R}$ we know that it must have a greatest lower bound, call it β, i.e. $\inf A = \beta$. Hence we have that $x \geq \beta \ \ \forall\, x \in A$. But then, this implies that $-x \leq -\beta \ \ \forall\, x \in A$. Thus, we have that $-\beta$ is an upper bound of $-A$. Now we show that it must in fact be the least upper bound.
For any $\varepsilon > 0$, we have

$$-\beta - \varepsilon = -(\beta + \varepsilon)$$

But then $\beta + \varepsilon$ is not a lower bound of A, since $\inf A = \beta$. Hence, it follows that $-\beta$ is in fact the least upper bound of $-A$. Thus, $\beta = \inf A = -(-\beta) = -\sup(-A)$. ■

(Alternate) Proof:
Suppose $A \subseteq \mathbb{R}$ is bounded below by β. That is, $\beta \leq x \ \ \forall\, x \in A$. Define $-A = \{-x : x \in A\}$. Then $-A$ is bounded above by $-\beta$. Let $\alpha = \sup(-A)$. Notice that $-x \leq \alpha \ \ \forall\, -x \in -A$. This means that $-\alpha \leq x \ \ \forall\, x \in A$. In particular, $-\alpha$ is a lower bound of A.
Let $\varepsilon > 0$, then $\alpha - \varepsilon$ is not an upper bound of $-A$ since there exists some $-x \in -A$ such that $\alpha - \varepsilon < -x \leq \alpha$. It follows that $-\alpha + \varepsilon > x \geq -\alpha$, which tells us that $-\alpha + \varepsilon$ is not a lower bound.
We thus conclude that $-\alpha$ is the greatest lower bound of A. That is, $\inf A = -\alpha = -\sup(-A)$. ■

(Alternate) Proof:
We need to prove that $-\sup(-A)$ is the greatest lower bound of A. For brevity, let $s = -\sup(-A)$.
We want to show that $s \leq x \ \ \forall\, x \in A$ and $s \geq t$ if t is any lower bound of A.
Suppose $x \in A$. Then, $-x \in -A$, and thus, $-x \leq \sup(-A)$. It follows that $x \geq -\sup(-A)$, i.e. $s \leq x$.
Thus s is a lower bound of A. Now let t be any lower bound of A. This means $t \leq x \ \ \forall\, x \in A$. Hence,

$-x \le -t \ \ \forall\, x \in A$, which says $y \le -t \ \ \forall\, y \in -A$. This means that $-t$ is an upper bound of $-A$. Hence $-t \ge \sup(-A)$ by definition of sup, i.e. $t \le -\sup(-A)$, and so $-\sup(-A)$ is the greatest lower bound of A. ■

(5) Fix $b > 1$. Then,

a) Let $m,\ n,\ p,\ q$ be integers, with $n,\ q > 0$ and $r = \frac{m}{n} = \frac{p}{q}$. Prove that

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

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

<u>Proof:</u>

Let $r = \frac{m}{n} = \frac{p}{q}$. Then $mq = np$ and $\left((b^m)^{1/n}\right)^{nq} = b^{mq} = b^{np} = \left((b^p)^{1/q}\right)^{nq}$.

Since roots are unique, it follows that $(b^m)^{1/n} = (b^p)^{1/q}$. Hence it makes sense to define $b^r = (b^m)^{1/n}$.

■

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

<u>Proof:</u>

Let $r = \frac{m}{n}$ and $s = \frac{c}{t}$. Then,

$(b^{r+s})^{nt} = b^{mt+nc} = b^{mt}\, b^{nc} = \left((b^{mt})^{1/nt}\right)^{nt} \left((b^{nc})^{1/nt}\right)^{nt} = (b^{m/n})^{nt} \left(b^{c/t}\right)^{nt} = (b^r)^{nt}\, (b^s)^{nt} = (b^r\, b^s)^{nt}$.

Since roots are unique, it follows that $b^{r+s} = b^r\, b^s$. ■

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

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

when r is rational. Hence it makes sense to define

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

for every real x.

<u>Proof:</u>

Let $s,\ t \in \mathbb{Q}$ wih $s < t$.

Then, $t - s = \frac{m}{n} > 0$ and

$$\left(\frac{b^t}{b^s}\right)^n = \left(b^{t-s}\right)^n = \left(b^{m/n}\right)^n = b^m\ .$$

Since $b > 1$, it follows that $b^m > b > 1$. We conclude that $(b^m)^{1/n} > 1$. Thus, $b^{t-s} > 1$ or, equivalently, $b^t > b^s$.

If we define $B(x) = \{b^t : t \in \mathbb{Q},\ t \leq x\}$, we obtain $b^r = \sup B(r)$, because for any $t < r$, we have $b^t < b^r$ and $b^r \in B(r)$. ■

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

Proof:
Let $b^p \in B(x)$ and $b^q \in B(y)$. Then $p, q \in \mathbb{Q}$ and $p < x,\ \ q < y$. It follows that $b^p\, b^q = b^{p+q} \in B(x+y)$. Therefore $\sup B(x)\ \sup B(y) \leq \sup B(x+y)$.
Let $t < x + y$. Then $t - x < y$. Since the rationals are dense on the real number line, there exists $s \in \mathbb{Q}$ such that $t - x < s < y$. Since $t - s < x$, there exists some $r \in \mathbb{Q}$ such that $t - s < r < x$. Hence $t < r + s < x + s < x + y$, where $r < x$ and $s < y$. Thus, $b^t < b^{r+s} = b^r\, b^s \leq \sup B(x)\ \sup B(y) = b^x\, b^y$.
In other words, $b^{x+y} = \sup B(x+y) \leq b^x\, b^y$.
Since $b^{x+y} \leq b^x\, b^y$ and $b^x\, b^y \leq b^{x+y}$, it follows that $b^{x+y} = b^x\, b^y$. ■

(6) Fix $b > 1,\ y > 0$, and prove that there is a unique real x such that $b^x = y$, by completing the following outline (This x is called the logarithm of y to the base b) :

a) For any positive integer n, $b^n - 1 \geq n(b-1)$.
Solution:
$b^n - 1 = (b-1)\,(b^{n-1} + b^{n-2} + \ldots + 1) > (b-1)\,(1 + 1 + \ldots + 1) = (b-1)\,n$. ✓

b) Hence $b - 1 \geq n(b^{1/n} - 1)$.
Solution:
Let $\alpha = b^{1/n}$. Then $\alpha^n - 1 > n(\alpha - 1)$ by part a) (since $\alpha > 1$). Now $\alpha^n = b$ and the inequality can be expressed as $b - 1 > n(b^{1/n} - 1)$. ✓

c) If $t > 1$ and $n > \frac{b-1}{t-1}$, then $b^{1/n} < t$.
Solution:
If $t > 1$ and $n > \frac{b-1}{t-1}$, then by part b), $n(t-1) > b - 1 > n(b^{1/n} - 1)$. The inequality $n(t-1) > n\,(b^{1/n} - 1)$ is equivalent to $t > b^{1/n}$. ✓

d) If w is such that $b^w < y$, then $b^{w+1/n} < y$ for sufficiently large n; to see this, apply part c) with $t = y\, b^{-w}$.
Solution:
Suppose $b^w < y$, then $y\, b^{-w} > 1$. Setting $t = y\, b^{-w}$ and $n > \frac{b-1}{t-1}$ yields $b^{1/n} < y\, b^{-w}$ (by part c)).
Therefore, $b^w\, b^{1/n} = b^{w+1/n} < y$. ✓

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

Solution:

Suppose $b^w > y$, then $y^{-1}\, b > 1$. Setting $t = y^{-1}\, b$ and $n > \frac{b-1}{t-1}$ yields $b^{1/n} < t = y^{-1}\, b$ (by part **c)**).
Therefore, $y < b^w\, b^{-1/n} = b^{w-1/n}$. ✓

f) Let A be the set of all w such that $b^w < y$, and show that $x = \sup A$ satisfies $b^x = y$.

Proof:

Let $A = \{w \in \mathbb{R} : b^w < y\}$. Then,

i) $A \neq \emptyset$:

If $y > 1$, set $n > \frac{b-1}{y-1}$ and use part c) to conclude that $b^{1/n} < y$.

In other words, if $y > 1$, $\frac{1}{n} \in A$. If $y = 1$, then $b^0 = 1 = y$, hence $0 \in A$. Finally, if $y < 1$, then $\frac{1}{y} > 1$ and setting $m > \frac{b-1}{\frac{1}{y} - 1}$ yields $b^{1/m} < \frac{1}{y}$ by part c). It follows that $y < b^{-1/m}$. In any case, A is not empty.

ii) A is bounded above:

Define $B = \{b^n : n \in \mathbb{N}\}$. Then B does not have an upper bound. To see why, assume instead that it does. Set $\sup B = s$. Since $b > 1$, $\frac{s}{b} < s$. In particular, $\frac{s}{b}$ is not an upper bound of B. There exists some $n \in \mathbb{N}$ such that $b^n > \frac{s}{b}$. But then $b^{n+1} > s$, which contradicts the assumption that $s = \sup B$. ($\Rightarrow\Leftarrow$)

It follows that B is not bounded above. This means that for some integer $k \in \mathbb{N}$, $b^k > y$. Since $w < k$ implies $b^w < b^k$ (and $b^w < b^k$ implies $w < k$), we see that A is bounded above by k.

Let $x = \sup A$. we wish to show that $b^x = y$.

If $b^x < y$, part d) implies that $b^{x+1/n} < y$ for some sufficiently large n. Thus, $b^x < b^{x+1/n} < y$ and $x + \frac{1}{n} \in A$ in contradiction to the assumption that $x = \sup A$.

If otherwise $b^x > y$, part e) implies that $b^{x-1/n} > y$ for some sufficiently large n. Thus, $x - \frac{1}{n}$ is an upper bound of A, which is not possible. ($\Rightarrow\Leftarrow$) ■

g) Prove that this x is unique.

Proof:

If α and β satisfy $b^\alpha = b^\beta = y$ then $\alpha = \beta$. This follows from the fact that if $\alpha < \beta$ then there are rationals r, s that satisfy $\alpha < r < s < \beta$. Thus $b^\alpha < b^r < b^s < b^\beta$ by the work done in the previous problem. It follows then that an x satisfying $b^x = y$ is unique. ■

(7) Let $p \geq 2$ be a fixed integer, and let $0 < x < 1$. If x has a finite-length base-p decimal expansion, that is, if $x = \frac{a_1}{p} + \ldots + \frac{a_n}{p^n}$ with $a_n \neq 0$, prove that x has precisely two base-p decimal expansions.

Otherwise, show that the base-p decimal expansion for x is unique.

Proof:
Suppose $x = \frac{a_1}{p} + \ldots + \frac{a_n}{p^n}$.
Then,

$$x = \frac{a_1}{p} + \ldots + \frac{a_n - 1}{p^n} + \sum_{i=n+1}^{\infty} \frac{p-1}{p^i} \qquad \left(\text{since } \frac{1}{p^n} = \sum_{i=n+1}^{\infty} \frac{p-1}{p^i}\right).$$

Let

$$0.\, b_1\, b_2 \ldots b_n \ldots \qquad \text{and} \qquad 0.\, c_1\, c_2 \ldots c_n \ldots$$

be any two base p decimal expansions for x and suppose n is the first integer for which $b_i \neq c_i$. Then, WLOG, $b_1 = c_1$, $b_2 = c_2$, ..., $b_{i-1} = c_{i-1}$, $b_n < c_n$.
Thus,

$$0.\, b_1\, b_2 \ldots b_n \ldots = \sum_{i=1}^{\infty} \frac{b_i}{p^i} \leq \sum_{i=1}^{n} \frac{b_i}{p^i} + \sum_{i=n+1}^{\infty} \frac{p-1}{p^i} = \frac{b_1}{p} + \frac{b_2}{p^2} + \ldots + \frac{b_n + 1}{p^n}$$

$$\leq \frac{c_1}{p} + \frac{c_2}{p^2} + \ldots + \frac{c_n}{p^n} \leq \sum_{i=1}^{\infty} \frac{c_i}{p^i} = 0.\, c_1\, c_2 \ldots c_n \ldots$$

with equality iff $b_{n+i} = p - 1$, $c_n = b_n + 1$, and $c_{n+i} = 0 \quad \forall\, i \geq 1$.
This means that if x has two decimal expansions, one of them must be finite. Hence, if x does not have a finite decimal expansion (mod p), its representation is unique. ■

(8) Prove that no order can be defined in the complex field that turns it into an ordered field. Hint: -1 is a square.

Proof:
If order is imposed on $\mathbb{C}$, then, for each $z \in \mathbb{C}$ $(z \neq 0)$, either $z > 0$ or $z < 0$.
Let $z = i$. By proposition 1.18(d) (Rudin's), $z^2 > 0$ for any $z \neq 0$.
Thus, $-1 = i^2 > 0$. However, since $1 = 1^2 > 0$ (again by 1.18(d)), it follows that both 1 and -1 are greater than 0. This violates proposition 1.18(a). Thus $\mathbb{C}$ cannot be an ordered field. ■

(9) Suppose $z = a + b\,i$, $w = c + d\,i$. Define $z < w$ if $a < c$, and also if $a = c$ but $b < d$. Prove that this turns the set of all complex numbers into an ordered set. (This type of order relation is called a dictionary order, or lexicographic order, for obvious reasons.) Does this ordered set have the least-upper-bound property?

Proof:
The proof that the lexicographic order turns $\mathbb{C}$ into an ordered set is trivial. To see whether or not $\mathbb{C}$ is transformed into a set with the least upper bound property, set $A = \{b\,i : b \in \mathbb{R}\}$. Then A is bounded above by any element $z \in \mathbb{C}$ for which $\mathrm{Re}(z) > 0$. Observe also that if $z = a + b\,i$ with

$a = \mathrm{Re}(z) \leq 0$, then $w = (|b| + 1)\, i \in A$ satisfies $w > z$.
Although A is bounded above, A does not have a l.u.b. To see this, suppose $\alpha + \beta\, i$ is an upper bound. Then $\alpha > 0$ and $\frac{\alpha}{2} + \beta\, i$ is also an upper bound with $\frac{\alpha}{2} + \beta\, i < \alpha + \beta\, i$. ■

(10) Suppose $z = a + b\, i$, $w = u + v\, i$, and

$$a = \sqrt{\frac{|w| + u}{2}}\ ,\quad b = \sqrt{\frac{|w| - u}{2}}$$

Prove that $z^2 = w$ if $v \geq 0$ and $(\bar{z})^2 = w$ if $v \leq 0$. Conclude that every complex number (with one exception!) has two complex square roots.

Proof:
Let $z = a + b\, i$ and $w = u + v\, i$.
Then $z^2 = w$ iff the equations

$$\text{(I)} \qquad a^2 - b^2 = u$$
$$\text{(II)} \qquad 2\, a\, b = v$$

are satisfied.
We now write $b = \frac{v}{2\, a}$ and plug it into (I) to obtain $a^2 - \frac{v^2}{4\, a^2} = u$. Now we take this result and multiply it by a^2 to obtain $a^4 - a^2\, u - \frac{v^2}{4} = 0$. From here we have $a^2 = \frac{u + \sqrt{u^2 + v^2}}{2}$. Now since $b^2 = u - a^2$ by (I), we have that $b^2 = \frac{-u + \sqrt{u^2 + v^2}}{2}$. Therefore $a^2 = \frac{|w| + u}{2}$ and $b^2 = \frac{|w| - u}{2}$, from which we obtain that $a = \pm\sqrt{\frac{|w| + u}{2}}$ and $b = \pm\sqrt{\frac{|w| - u}{2}}$.

If $v > 0$ then

$$2\sqrt{\frac{|w| + u}{2}}\ \sqrt{\frac{|w| - u}{2}} = 2\sqrt{\frac{|w|^2 - u^2}{4}} = 2\sqrt{\frac{v^2}{4}} = |v| = v\,.$$

Similarly,

$$2\left(-\sqrt{\frac{|w| + u}{2}}\right)\left(-\sqrt{\frac{|w| - u}{2}}\right) = v \quad \text{if } v > 0\,.$$

Thus $|a| + |b|\, i$ and $-(|a| + |b|\, i)$ are solutions to the equation $z^2 = w$ in this case.

If $v < 0$, then $-|a| + |b|\, i$ and $|a| - |b|\, i$ are solutions to $z^2 = w$.

We see that if $w \neq 0$ the equation $z^2 = w$ has at least two solutions. It can be shown that a polynomial equation of degree n can have at most n solutions. In particular, $z^2 - w = 0$ can have at most two solutions. Thus, if $w \neq 0$, the equation $z^2 = w$ has exactly two solutions. ■

(11) If z is a complex number, prove that there exists an $r \geq 0$ and a complex number w with $|w| = 1$, such that $z = r\,w$. Are w and r always uniquely determined by z?

Proof:
Let $z \neq 0$ and set $r = |z|$ and $w = \frac{z}{|z|}$, so that $|w| = 1$ and $r > 0$. Clearly, $z = r\,w$.
To see that z determines r and w uniquely, suppose $z = p\,u$, where $p > 0$ and $|u| = 1$. Then $|z| = |p\,u| = |p|\,|u| = p$. But $|z| = r$. Hence, $p = r$. Now $\frac{1}{r}\,z = \frac{1}{r}\,p\,u = \frac{1}{r}\,r\,w$. Thus, it follows that $u = w$.
* Remark: If $z = 0$, $z = r\,w$ when $r = 0$ and $|w| = 1$. * ■

(12) If z_1, .., z_n are complex, prove that

$$|z_1 + \ldots + z_n| \leq |z_1| + \ldots + |z_n| \,.$$

Proof:
This follows from repeatedly applying theorem 1.33 (e) (Rudin's). ■

(13) If z is a complex number such that $|z| = 1$, i.e. $z\,\overline{z} = 1$, compute

$$|1 + z|^2 + |1 - z|^2 \,.$$

Solution:
Suppose $z\,\overline{z} = 1$. Then

$$\begin{aligned} |1 + z|^2 + |1 - z|^2 &= (1 + z)\,\overline{(1 + z)} + (1 - z)\,\overline{(1 - z)} = (1 + z)\,(1 + \overline{z}) + (1 - z)\,(1 - \overline{z}) \\ &= (1 + \overline{z} + z + z\,\overline{z}) + (1 - \overline{z} - z + z\,\overline{z}) = (2 + \overline{z} + z) + (2 - \overline{z} - z) \\ &= 4 \,. \end{aligned}$$