Week 6 Problems

Muhammad Meesum Ali Qazalbash

October 20, 2022

Question:	1	2	3	4	5	6	7	8	9	10	11	Total
Points:	1	1	1	1	1	1	1	1	1	1	1	11
Score:												

1. (1 point) $\mathbf{Z}_5$ is the set $\{0, 1, 2, 3, 4\}$ with arithmetic done modulo 5, that is, do the usual operations and then subtract 5 repeatedly until the result is an element of the set. We can do arithmetic modulo any natural number greater than 1, so $3+4 = 2(\mathrm{mod}\,5)$, $5\times 6 = 6(\mathrm{mod}\,8)$, and $9 \times 8 = 0(\mathrm{mod}\,12)$, for example.
   (a) Show that $\mathbf{Z}_5$ (or $\mathbf{Z}_3$ or $\mathbf{Z}_7$) is a field.

Solution: First we will introduce some properties of modulo (we will not prove them),

$$(a+b)(\mathrm{mod}\,n) = (a(\mathrm{mod}\,n) + b(\mathrm{mod}\,n))(\mathrm{mod}\,n)$$
$$(a\times b)(\mathrm{mod}\,n) = (a(\mathrm{mod}\,n) \times b(\mathrm{mod}\,n))(\mathrm{mod}\,n)$$

With these properties we can reduce numbers greater than 4 to any one number in the set $\mathbf{Z}_5$. The addition and multiplication table of the field $\mathbf{Z}_5$ are below,

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Each number in addition table is in $\mathbf{Z}_5$. Addition by 0 does not change the number means it is the additive identity. There is only one 0 in every row or column in addition table that means there exist a unique additive inverse for every number in $\mathbf{Z}_5$. Addition is associative. Similarly, the multiplication is closed, there is a unique multiplicative identity, every number has multiplicative inverse along with associativity.

$$\begin{aligned}(a\times(b+c))(\mathrm{mod}\,5) &= (a\times b + a\times c)(\mathrm{mod}\,5)\\ &= ((a\times b)(\mathrm{mod}\,5) + (a\times c)(\mathrm{mod}\,5))(\mathrm{mod}\,5)\end{aligned}$$

This means distributive property also holds over this set with addition and multiplication. Hence, $(\mathbf{Z}_5, +, \times)$ is a field. ■

(b) Show that $\mathbf{Z}_4$ (or $\mathbf{Z}_6$ or $\mathbf{Z}_{14}$) is *not* a field.

Solution: We will show $\mathbf{Z}_4$ is not a field. The multiplication table will be,

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

We can see that there is no inverse of 2 in $\mathbf{Z}_4$. Hence, $(\mathbf{Z}_4, +, \times)$ is not a field.

(c) For which values of n is $\mathbf{Z}_n$ a field? State and prove a theorem.

Solution:

Statement 0.1 *If n is a prime number then $(\mathbf{Z}_n, +, \times)$ is a field*

We will prove this with contradiction. We assume that n is a composite number and $(\mathbf{Z}_n, +, \times)$ is a field. We know that every composite number can be expressed as a product of some primes i.e. $n = p_1 \times p_2 \times \cdots \times p_m$. It is trivial that $\forall i, p_i < n$, therefore, $p_i \in \mathbf{Z}_n$.

$$\begin{aligned} n &= p_1 \times p_2 \times \cdots \times p_m \\ n (\mathrm{mod}\, n) &\equiv p_1 \times p_2 \times \cdots \times p_m (\mathrm{mod}\, n) \\ 0 (\mathrm{mod}\, n) &\equiv p_1 \times p_2 \times \cdots \times p_m (\mathrm{mod}\, n) \end{aligned}$$

$(\mathbf{Z}_n, +, \times)$ is a field,$\therefore \exists p_1^{-1} \in \mathbf{Z}_n$. We will multiply it on both sides,

$$\begin{aligned} p_1^{-1} \times 0 (\mathrm{mod}\, n) &\equiv p_1^{-1} \times p_1 \times p_2 \times \cdots \times p_m (\mathrm{mod}\, n) \\ 0 (\mathrm{mod}\, n) &\equiv (p_1^{-1} \times p_1) \times p_2 \times \cdots \times p_m (\mathrm{mod}\, n) \\ 0 (\mathrm{mod}\, n) &\equiv 1 \times p_2 \times \cdots \times p_m (\mathrm{mod}\, n) \\ 0 (\mathrm{mod}\, n) &\equiv p_2 \times \cdots \times p_m (\mathrm{mod}\, n) \end{aligned}$$

$$\because p_2 \times \cdots \times p_m < n \implies 0 (\mathrm{mod}\, n) \not\equiv p_2 \times \cdots \times p_m (\mathrm{mod}\, n)$$

Hence our asssumption was wrong. If n is a prime number then $(\mathbf{Z}_n, +, \times)$ is a field. ■

2. (1 point) (a) Let $\mathbb{F}$ be the set of all real numbers of the form $a + b\sqrt{2}$, where a and b are rational numbers. Show that $\mathbb{F}$ is a field.

Solution: Let $w, w_1, w_2, w_3 \in \mathbb{F}$ such that $w = a + b\sqrt{2}$ and for $i = 1, 2, 3$, $w_i = a_i + b_i\sqrt{2}$, where $a_i, b_i \in \mathbb{Q}$.

Closure

$$\begin{aligned} w_1 + w_2 &= (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \\ &\in \mathbb{F} \\ w_1 \times w_2 &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \\ &\in \mathbb{F} \end{aligned}$$

Commutativity

$$\begin{aligned} w_1 + w_2 &= (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \\ &= (a_2 + a_1) + (b_2 + b_1)\sqrt{2} \\ &= (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2}) \\ &= w_2 + w_1 \\ w_1 \times w_2 &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \\ &= (a_2a_1 + 2b_2b_1) + (a_2b_1 + a_1b_2)\sqrt{2} \\ &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= w_2 \times w_1 \end{aligned}$$

Associativity

$$\begin{aligned} w_1 + (w_2 + w_3) &= (a_1 + b_1\sqrt{2}) + ((a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{2})) \\ &= (a_1 + b_1\sqrt{2}) + ((a_2 + a_3) + (b_2 + b_3)\sqrt{2}) \\ &= (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2} \\ &= ((a_1 + a_2) + (b_1 + b_2)\sqrt{2}) + (a_3 + b_3\sqrt{2}) \\ &= (w_1 + w_2) + w_3 \\ w_1 \times (w_2 \times w_3) &= (a_1 + b_1\sqrt{2})((a_2 + b_2\sqrt{2})(a_3 + b_3\sqrt{2})) \\ &= (a_1 + b_1\sqrt{2})((a_2a_3 + 2b_2b_3) + (a_2b_3 + a_3b_2)\sqrt{2}) \\ &= (a_1a_2a_3 + 2a_1b_2b_3 + 2a_2b_1b_3 + 2a_3b_1b_2) \\ &\quad + (a_1a_2b_3 + a_1a_3b_2 + a_2a_3b_1 + 2b_1b_2b_3)\sqrt{2} \\ &= ((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2})(a_3 + b_3\sqrt{2}) \\ &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})(a_3 + b_3\sqrt{2}) \\ &= (w_1 \times w_2) \times w_3 \end{aligned}$$

Indentities

$$\begin{aligned} w + 0 &= (a + b\sqrt{2}) + 0 \\ &= (a + b\sqrt{2}) + (0 + 0\sqrt{2}) \\ &= (a + 0) + (b + 0)\sqrt{2} \\ &= w \\ w \times 1 &= (a + b\sqrt{2}) \times 1 \\ &= (a + b\sqrt{2})(1 + 0\sqrt{2}) \\ &= (a(1) + 2b(0)) + (a(0) + (1)b)\sqrt{2} \\ &= a + b\sqrt{2} \\ &= w \end{aligned}$$

Inverses

$$\begin{aligned} -w &= -a - b\sqrt{2} \\ \implies w + (-w) &= (a + b\sqrt{2}) + (-a - b\sqrt{2}) \\ &= (a + (-a)) + (b + (-b))\sqrt{2} \\ &= 0 + 0\sqrt{2} \\ &= 0 \\ w^{-1} &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ \implies w \times w^{-1} &= \frac{(a + b\sqrt{2})(a - b\sqrt{2})}{a^2 - 2b^2} \\ &= \frac{(a^2 - 2b^2) + (ab - ab)\sqrt{2}}{a^2 - 2b^2} \\ &= 1 + 0\sqrt{2} \\ &= 1 \end{aligned}$$

Distributivity

$$\begin{aligned} w_1(w_2 + w_3) &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2} + a_3 + b_3\sqrt{2}) \\ &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2})(a_3 + b_3\sqrt{2}) \\ &= w_1 \times w_2 + w_1 \times w_3 \end{aligned}$$

Hence, $\mathbb{F}$ is a field. ■

(b) If $k > 0$ is a rational number that doesn't have a rational square root, show that the set $\{a + b\sqrt{k} : a, b \in \mathbb{Q}\}$ is a field.

Solution: Let $w, w_1, w_2, w_3 \in \mathbb{F}$ such that $w = a + b\sqrt{k}$ and for $i = 1, 2, 3$, $w_i = a_i + b_i\sqrt{k}$, where $a_i, b_i \in \mathbb{Q}$.

Closure

$$\begin{aligned} w_1 + w_2 &= (a_1 + b_1\sqrt{k}) + (a_2 + b_2\sqrt{k}) \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{k} \\ &\in \mathbb{F} \\ w_1 \times w_2 &= (a_1 + b_1\sqrt{k})(a_2 + b_2\sqrt{k}) \\ &= (a_1a_2 + kb_1b_2) + (a_1b_2 + a_2b_1)\sqrt{k} \\ &\in \mathbb{F} \end{aligned}$$

Commutativity

$$\begin{aligned} w_1 + w_2 &= (a_1 + b_1\sqrt{k}) + (a_2 + b_2\sqrt{k}) \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{k} \\ &= (a_2 + a_1) + (b_2 + b_1)\sqrt{k} \\ &= (a_2 + b_2\sqrt{k}) + (a_1 + b_1\sqrt{k}) \\ &= w_2 + w_1 \\ w_1 \times w_2 &= (a_1 + b_1\sqrt{k})(a_2 + b_2\sqrt{k}) \\ &= (a_1a_2 + kb_1b_2) + (a_1b_2 + a_2b_1)\sqrt{k} \\ &= (a_2a_1 + kb_2b_1) + (a_2b_1 + a_1b_2)\sqrt{k} \\ &= (a_1 + b_1\sqrt{k})(a_2 + b_2\sqrt{k}) \\ &= w_2 \times w_1 \end{aligned}$$

Associativity

$$\begin{aligned} w_1 + (w_2 + w_3) &= (a_1 + b_1\sqrt{k}) + ((a_2 + b_2\sqrt{k}) + (a_3 + b_3\sqrt{k})) \\ &= (a_1 + b_1\sqrt{k}) + ((a_2 + a_3) + (b_2 + b_3)\sqrt{k}) \\ &= (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{k} \\ &= ((a_1 + a_2) + (b_1 + b_2)\sqrt{k}) + (a_3 + b_3\sqrt{k}) \\ &= (w_1 + w_2) + w_3 \\ w_1 \times (w_2 \times w_3) &= (a_1 + b_1\sqrt{k})((a_2 + b_2\sqrt{k})(a_3 + b_3\sqrt{k})) \\ &= (a_1 + b_1\sqrt{k})((a_2a_3 + kb_2b_3) + (a_2b_3 + a_3b_2)\sqrt{k}) \\ &= (a_1a_2a_3 + ka_1b_2b_3 + ka_2b_1b_3 + ka_3b_1b_2) \\ &\quad + (a_1a_2b_3 + a_1a_3b_2 + a_2a_3b_1 + kb_1b_2b_3)\sqrt{k} \\ &= ((a_1a_2 + kb_1b_2) + (a_1b_2 + a_2b_1)\sqrt{k})(a_3 + b_3\sqrt{k}) \\ &= (a_1 + b_1\sqrt{k})(a_2 + b_2\sqrt{k})(a_3 + b_3\sqrt{k}) \\ &= (w_1 \times w_2) \times w_3 \end{aligned}$$

Indentities

$$\begin{aligned} w + 0 &= (a + b\sqrt{k}) + 0 \\ &= (a + b\sqrt{k}) + (0 + 0\sqrt{k}) \\ &= (a + 0) + (b + 0)\sqrt{k} \\ &= w \\ w \times 1 &= (a + b\sqrt{k}) \times 1 \\ &= (a + b\sqrt{k})(1 + 0\sqrt{k}) \\ &= (a(1) + kb(0)) + (a(0) + (1)b)\sqrt{k} \\ &= a + b\sqrt{k} \\ &= w \end{aligned}$$

Inverses

$$\begin{aligned} -w &= -a - b\sqrt{k} \\ \implies w + (-w) &= (a + b\sqrt{k}) + (-a - b\sqrt{k}) \\ &= (a + (-a)) + (b + (-b))\sqrt{k} \\ &= 0 + 0\sqrt{k} \\ &= 0 \\ w^{-1} &= \frac{a - b\sqrt{k}}{a^2 - kb^2} \\ \implies w \times w^{-1} &= \frac{(a + b\sqrt{k})(a - b\sqrt{k})}{a^2 - kb^2} \\ &= \frac{(a^2 - kb^2) + (ab - ab)\sqrt{k}}{a^2 - kb^2} \\ &= 1 + 0\sqrt{k} \\ &= 1 \end{aligned}$$

Distributivity

$$\begin{aligned} w_1(w_2 + w_3) &= (a_1 + b_1\sqrt{k})(a_2 + b_2\sqrt{k} + a_3 + b_3\sqrt{k}) \\ &= (a_1 + b_1\sqrt{k})(a_2 + b_2\sqrt{k}) + (a_1 + b_1\sqrt{k})(a_3 + b_3\sqrt{k}) \\ &= w_1 \times w_2 + w_1 \times w_3 \end{aligned}$$

Hence, $\mathbb{F}$ is a field. ■

(c) If the number k in 2b does have a rational square root, show that the set constructed is just $\mathbb{Q}$.

Solution:

$$\exists t \in \mathbb{Q} \ni \sqrt{k} = t \implies \forall w = a + bt \in \mathbb{F}, w \in \mathbb{Q}$$

This means the field is actually $\mathbb{Q}$. ■

(d) Suppose k is a rational number that doesn't have a rational square root (this time, k might be negative). We endow the symbol with the property that $2 = k$. Show that the collection of symbols $a + b$ is a field (note that they may not be real numbers). Here multiplication and addition are carried out as if were a variable, with $\diamond^2$ replaced by k whenever it appears. For instance, we would have:

$$(1 + \diamond)(2 + \diamond) = 2 + 3 \diamond + k$$

Solution: Let $w, w_1, w_2, w_3 \in \mathbb{F}$ such that $w = a + b\diamond$ and for $i = 1, 2, 3$, $w_i = a_i + b_i\diamond$, where $a_i, b_i \in \mathbb{Q}$.

Closure

$$\begin{aligned} w_1 + w_2 &= (a_1 + b_1\diamond) + (a_2 + b_2\diamond) \\ &= (a_1 + a_2) + (b_1 + b_2)\diamond \\ &\in \mathbb{F} \\ w_1 \times w_2 &= (a_1 + b_1\diamond)(a_2 + b_2\diamond) \\ &= (a_1a_2 + kb_1b_2) + (a_1b_2 + a_2b_1)\diamond \\ &\in \mathbb{F} \end{aligned}$$

Commutativity

$$\begin{aligned} w_1 + w_2 &= (a_1 + b_1\diamond) + (a_2 + b_2\diamond) \\ &= (a_2 + a_1) + (b_2 + b_1)\diamond \\ &= w_2 + w_1 \\ w_1 \times w_2 &= (a_1 + b_1\diamond)(a_2 + b_2\diamond) \\ &= (a_1a_2 + kb_1b_2) + (a_1b_2 + a_2b_1)\diamond \\ &= (a_2a_1 + kb_2b_1) + (a_2b_1 + a_1b_2)\diamond \\ &= (a_2 + b_2\diamond)(a_1 + b_1\diamond) \\ &= w_2 \times w_1 \end{aligned}$$

Associativity

$$\begin{aligned} w_1 + (w_2 + w_3) &= (a_1 + b_1\diamond) + ((a_2 + b_2\diamond) + (a_3 + b_3\diamond)) \\ &= (a_1 + b_1\diamond) + ((a_2 + a_3) + (b_2 + b_3)\diamond) \\ &= (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\diamond \\ &= ((a_1 + a_2) + (b_1 + b_2)\diamond) + (a_3 + b_3)\diamond \\ &= ((a_1 + b_1\diamond) + (a_2 + b_2\diamond)) + (a_3 + b_3)\diamond \\ &= (w_1 + w_2) + w_3 \end{aligned}$$

Indentities

$$\begin{aligned} w + 0 &= (a + b\diamond) + 0 \\ &= (a + b\diamond) + (0 + 0\diamond) \\ &= (a + 0) + (b + 0)\diamond \\ &= w \\ w \times 1 &= (a + b\diamond) \times 1 \\ &= (a + b\diamond)(1 + 0\diamond) \\ &= (a(1) + k(0)) + (a(0) + (1)b)\diamond \\ &= a + b\diamond \\ &= w \end{aligned}$$

Inverses

$$\begin{aligned} -w &= -a - b\diamond \\ \implies w + (-w) &= (a + b\diamond) + (-a - b\diamond) \\ &= (a + (-a)) + (b + (-b))\diamond \\ &= 0 + 0\diamond \\ &= 0 \\ w^{-1} &= \frac{a - b\diamond}{a^2 - kb} \\ \implies w \times w^{-1} &= \frac{(a + b\diamond)(a - b\diamond)}{a + b\diamond} \\ &= \frac{(a^2 - k) + (ab - ab)\diamond}{a^2 - kb} \\ &= 1 + 0\diamond \\ &= 1 \end{aligned}$$

3. (1 point) If S is a subset of an ordered set, a least element of S is an element x, if there is one, such that (i) $x \in S$ and (ii) if $y \in S$ and y is comparable to x, then $x \leq y$.

   (a) Show that a subset of a linearly ordered set can have at most one least element.

   Solution: Let S be a subset of a linearly ordered set. Let x and y be least elements of S. Then $x \leq y$ and $y \leq x$. Since S is linearly ordered, $x = y$. ■

   (b) Show that in an ordering that is not linear a set can more than one least element.

   Solution: Let S be a subset of a non-linearly ordered set. Let x and y be least elements of S. Then $x \leq y$ and $y \leq x$. Since S is not linearly ordered, $x \neq y$. ■

   (c) Show that a subset of a linearly ordered set might not have a least element.

   Solution: $\mathbb{R}$ is linearly ordered by $\leq$. Let $\mathbb{R}^- \subseteq \mathbb{R}$, but there is no least element of $\mathbb{R}^-$. ■

4. (1 point) (a) How many ways are there to impose an ordering on a set with two elements? Three elements? N elements?

   Solution: If $p(n)$ is the function yields how many ordering are possible in a set that contains n elements, then the generating function is,

   $$\sum_{n \in \mathbb{N}} p(n)x^n = \prod_{k \in \mathbb{N}} \frac{1}{1 - x^k}$$

   Some of the initial values of the generating function are $1, 2, 3, 5, 7, 11, \cdots$.

   (b) How many of these orderings are linear?

   Solution: There are $N!$ ways of ordering a set with N elements. ■

5. (1 point) If we agree that the denominators used in representing rational numbers should always be positive, their usual ordering is given by

   $$\frac{p}{q} < \frac{r}{s} \iff ps < qr$$

   Show that this is a linear ordering.

   Solution: We can prove that $<$ is a strict-partial order over $\mathbb{Z}$ that means its ireflexive, asymmetric and transitive. $\forall a, b, c \in \mathbb{Z}$

   $$a \not< a$$
   $$a < b \implies b \not< a$$
   $$a < b \wedge b < c \implies a < c$$

If $m, n \in \mathbb{N}$,we say $m < n$ iff n is an element of the form $m+1, m+1+1, m+1+1+1, \cdots$. We will prove this using induction, our propostional function is,

$$P(q) : m < m + \sum_{i=1}^{q} 1$$

For base case, $q = 1$,$P(1) : m < m + 1$

Hypothesis is, $P(q) : m < m + \sum_{i=1}^{q} 1$

Inductive Step is,

$$\begin{aligned} P(q) : m < m + \sum_{i=1}^{q} 1 &\implies m + 1 < m + \sum_{i=1}^{q} 1 + 1 \\ &\implies m < m + 1 < m + \sum_{i=1}^{q+1} 1 \\ &\implies P(q+1) : m < m + \sum_{i=1}^{q+1} 1 \end{aligned}$$

Hence, if n is of form $m + \sum_{i=1}^{q} 1$, where q is any integer, then $m < n$.

We can use the same argument to prove that if $m < n$ then n must be a of a form $m+\sum_{i=1}^{q} 1$. We know that $m < m+1$ and with transitive property $m < m+\sum_{i=1}^{q}$, where q is any integer. Then there must be some q for which $m + \sum_{i=1}^{q-1} 1 < n < m + \sum_{i=1}^{q+1}$, this simply means if we keep on adding 1 then for some q we will get n. Hence, $m < n$.

Now we know that $<$ is a strict-partial order over $\mathbb{Z}$. Now we will prove that it is also a total order over $\mathbb{Z}$. $\forall a.b \in \mathbb{Z}$, we have two cases to consider.

1. If the two numbers are same then they can be compared as $a = b$.
2. If they are not equal then one must be less than other, we can compare them as, $a < b$ or $b > a$.

Hence, $<$ is a total order over $\mathbb{Z}$. In the question we have been given that the denominators used in representing rational numbers should always be positive and by the equivalence given $<$ is the total order over $\mathbb{Z}$, so we can say that $<$ is a total order over $\mathbb{Q}$. ■

6. (1 point) (a) Show that the following expression is an integer for $n = 0, 1, \ldots$

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Solution: Let the expression be x_n, then $x_0 = 0$ and $x_1 = 1$. Let $x_i \in \mathbb{Z}$ for some $i \leq k$, where $k \in \mathbb{N}$. We will use strong induction to show that $\bigwedge_{i=1}^{k} x_i \in \mathbb{Z} \implies x_{k+1} \in \mathbb{Z}$. Before that, if $\varphi = \frac{1+\sqrt{5}}{2}$ then $\varphi^2 = \varphi + 1$. Then the equation becomes,

$$\begin{aligned}
x_{k+1} &= \frac{\varphi^{k+1} - (-\varphi)^{-k-1}}{\sqrt{5}} \\
&= \frac{\varphi^{k-1}\varphi^2 - (-\varphi)^{-k+1}\varphi^{-2}}{\sqrt{5}} \\
&= \frac{\varphi^{k-1}(1+\varphi) - (-\varphi)^{-k+1}\left(1 - \frac{1}{\varphi}\right)}{\sqrt{5}} \\
&= \frac{\varphi^{k-1} + \varphi^k - (-\varphi)^{-k+1} - (-\varphi)^{-k}}{\sqrt{5}} \\
&= \frac{\varphi^k - (-\varphi)^{-k}}{\sqrt{5}} + \frac{\varphi^{k-1} - (-\varphi)^{-k+1}}{\sqrt{5}} \\
&= x_k + x_{k-1}
\end{aligned}$$

F By hypothesis x_k and x_{k-1} are integers, and sum of two integers is also an integer. Therefore x_{k+1} is also an integer. Hence $\forall n \in \mathbb{N}, x_n \in \mathbb{Z}$. ■

(b) If x_n is the expression in (a), show that

$$\lim_{n\to\infty} \frac{x_{n+1}}{x_n} = \frac{1+\sqrt{5}}{2}$$

Solution:

$$\begin{aligned}
\lim_{n\to\infty} \frac{x_{n+1}}{x_n} &= \lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}{\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n}} \\
&= \frac{1+\sqrt{5}}{2} \lim_{n\to\infty} \frac{1 - \left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^{n+1}}{1 - \left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^{n}} \\
&= \frac{1+\sqrt{5}}{2}\frac{1-0}{1-0} \\
&= \frac{1+\sqrt{5}}{2}
\end{aligned}$$

7. (1 point) Let $P(n)$ be the statement "$n^2 + 9n + 5$ is even."

   (a) Show that $P(k) \implies P(k+1)$ for $k \geq 1$.

   Solution:

   $$P(k+1) : (k+1)^2 + 9(k+1) + 5 = k^2 + 2k + 1 + 9k + 9 + 5$$
   $$= (k^2 + 9k + 5) + 2(k+5)$$

   Since, $k^2 + 9k + 5$ is even, we know that $2(k+5)$ is also even, therefore $P(k+1)$ is also even. ■

   (b) For which n is $P(n)$ true?

   Solution: It is true for no $n \in \mathbb{N}$.

   (c) What went wrong?

   Solution: The base case i.e. $P(1)$ is false. Therefore we can get any result we want by applying the induction hypothesis.

8. (1 point) (a) Show that $1 + 3 + \cdots + (2n-1) = n^2$ for $n = 1, 2, \cdots$

   Solution: We will prove this proposition with induction. Let

   $$P(n) : \sum_{i=1}^{n} (2i - 1) = n^2$$

   Then $P(1)$ is true. Let $P(k)$ be true for some $k \in \mathbb{N}$. Then

   $$\sum_{i=1}^{k+1} (2i-1) = \sum_{i=1}^{k} (2i-1) + 2k + 1 = k^2 + 2k + 1 = (k+1)^2$$

   Therefore $P(k+1)$ is also true. Hence $P(n)$ is true for all $n \in \mathbb{N}$. ■

(b) Show that $\frac{1}{1\times 2}+\frac{1}{2\times 3}+\cdots+\frac{1}{(n-1)\times n}=\frac{n}{n+1}$ for $n=1,2,\cdots$

Solution: We will prove this proposition with induction. Let

$$P(n):\sum_{i=0}^{n-1}\frac{1}{(i+1)\times(i+2)}=\frac{n}{n+1}$$

Then $P(1)$ is true. Let $P(k)$ be true for some $k\in\mathbb{N}$. Then

$$\begin{aligned}\sum_{i=0}^{k}\frac{1}{(i+1)\times(i+2)}&=\sum_{i=0}^{k-1}\frac{1}{(i+1)\times(i+2)}+\frac{1}{(k+1)\times(k+2)}\\&=\frac{k}{k+1}+\frac{1}{(k+1)\times(k+2)}\\&=\frac{(k+1)}{(k+1)+1}\end{aligned}$$

Therefore $P(k+1)$ is also true. Hence $P(n)$ is true for all $n\in\mathbb{N}$. ■

9. (1 point) In the complex numbers, we say the distance from $a+bi$ to 0 is. We might define an ordering on $\mathbb{C}$ by saying $z<w$ if it is closer to 0. Show that this does not make $\mathbb{C}$ into an ordered field.

Solution: Let $z,-z\in\mathbb{C}$, we know that these two complex numbers are diagonallay opposite on the circle they lie. Therefore there distance from the orgin is the same. Which means they can not be compared according to the scheme given in the question. Hence the scheme in the question can not order $\mathbb{C}$. ■

10. (1 point) Show that the field of rational numbers has the following property: Given any rational number $r=\frac{p}{q}$, there is a natural number n_r with $r<n_r$. (This is not difficult. Simply construct n_r from r.) An ordered field in which the natural numbers are distributed in this way is said to have the Archimedean property.

Solution: $\lceil x\rceil$ is a function that returns the smallest integer greater than or equal to x.

$$\forall x\in\mathbb{Q}, x\le\lceil x\rceil<\lceil x\rceil+1\implies x<\lceil x\rceil+1$$

$$r=\frac{p}{q}\implies\exists n_r=\lceil r\rceil+1\in\mathbb{N}\ni r<n_r$$

Hence the field of rational numbers has the Archimedean property. ■

11. (1 point) Can a field be ordered in more than one way? That is, can there be two sets $P_1 \neq P_2$ that both satisfy the definition of a positive set?

Solution: Let $\mathbb{F} = \mathbb{Q}(x)$, Any element of $\mathbb{F}$ can be written in the form,

$$f = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}$$

with $a_n, b_m \in \mathbb{R}/\{0\}$. Let $\mathbb{P} \subset \mathbb{F}$ be defined by the condition $f \in \mathbb{P} \iff \frac{a_n}{b_m} > 0$, and define $f \prec g \iff g - f \in \mathbb{P}$, then $(\mathbb{F}, \prec)$ is an ordered field.

We can define another order on $\mathbb{Q}(x)$. Let $\alpha \in \mathbb{R}$, where α is a transcendental real number i.e. it is not a solution of any algebric equation. Map $x \longmapsto \alpha$, and uses the order $<$ inherited from the reals. ■