HOMEWORK 2

SHUANGLIN SHAO

1. P63, Ex. 1

Proof. We prove it by contradiction. Assume that there exists a rational number r such that $r^2 = 3$ and $r > 0$. Since r is a rational number, then there exists $r = \frac{p}{q}$ such that $(p, q) = 1$, where the notation $(a, b) = 1$ means that the greatest common divisor of a and b is 1. Then

$$p^2 = 3q^2.$$

That is to say, p^2 is a multiple of 3. We may classify p in the following cases,

$$p = 3k, p = 3k + 1, p = 3k + 2, \text{ for integers } k.$$

In the latter two cases

$$p^2 = 9k^2 + 12k + 4, \, p^2 = 9k^2 + 12k + 4,$$

which are not multiples of 3. So $p = 3k$. Then we have

$$q^2 = 3k^2,$$

so by the reasoning above, q is a multiple of 3. This implies that 3 is a common divisor of p and q, which leads to a contradiction to $(p, q) = 1$. □

2. P63, Ex. 3

Proof. We prove it by contradiction. Assume that there exists a rational number r such that $r^3 = 2$ and $r > 0$. Since r is a rational number, then there exists $r = \frac{p}{q}$ such that $(p, q) = 1$ Then

$$p^3 = 2q^3.$$

That is to say, p^3 is a multiple of 2. We may classify p in the following cases,

$$p = 2k, p = 2k + 1, \text{ for integers } k.$$

In the latter two case

$$p^3 = 8k^3 + 12k^2 + 6k + 1,$$

which is not a multiple of 2. So $p = 2k$. Then we have

$$q^2 = 4k^2,$$

so by the reasoning above, q is a multiple of 2. This implies that 2 is a common divisor of p and q, which leads to a contradiction to $(p, q) = 1$. $\square$

3. P64, Ex. 8

Proof. We prove it by contradiction. Assume that there exists a rational number r such that $r^2 = 6$ and $r > 0$. Since r is a rational number, then there exists $r = \frac{p}{q}$ such that $(p, q) = 1$ Then

$$p^2 = 6q^2.$$

That is to say, p^2 is a multiple of 6. We may classify p in the following cases,

$$p = 6k, p = 6k + 1, 6k + 2, 6k + 3, 6k + 4, 6k + 5 \text{ for integers } k.$$

In the latter five case

$$p^2 = 36k^2+12k+1, 36k^2+24k+4, 36k^2+36k+9, 36k^2+48k+16, 36k^2+60k+25.$$

which are not multiples of 6. So $p = 6k$. Then we have

$$q^2 = 6k^2,$$

so by the reasoning above, q is a multiple of 6. This implies that 6 is a common divisor of p and q, which leads to a contradiction to $(p, q) = 1$. $\square$

4. P64, Ex. 9

Proof. We prove it by contradiction. Assume that $r = \sqrt{2}+\sqrt{3}$ is a rational number. Then $r^2 = 5 + 2\sqrt{6}$ is also a rational number. Then $\frac{r^2-5}{2} = \sqrt{6}$ should be a rational number, too. But Ex. 8 shows that it is an irrational number. So $\sqrt{2} + \sqrt{3}$ is an irrational number. $\square$

5. P75-76, Ex. 1.

In the following reasoning, we denote L the greatest lower bound and U the least upper bound of the sequence.

a) $U = 1$ and $L = 0$. U is in the set but L is not.
b) $U = 10$ and $L = 1$. Both numbers are not in the set.
c) $U = 10$ and $L = -1$. U is not in the set but L is in the set.
d) $U = \frac{1}{2}$ and $L = -1$. Both numbers are in the set.
e) $U = \sqrt{2}$ is not in the set. L does not exist.
f) $U = -\sqrt{3}$ is in the set but U does not exist.
r) $U = 0.1$ is in the set and $L = 0$ is not.
t) $U = 2$ is in the set but $L = 1$ is not.

v) $U = 1$ and $L = -1$ both numbers are not in the set.

6. P76. Ex. 2

Proof. Let a and b be the greatest lower bounds of the set A, where A is given as a nonempty bounded sets of $\mathbb{R}$. Since a is the greatest lower bound, and b is a lower bound,

$$a \geq b;$$

On the other hand, since b is the greatest lower bound, and a is a lower bound,

$$b \geq a.$$

These two inequalities imply

$$a = b.$$

□

7. P76. Ex. 4

Proof. The proof follows by verifying the seven rules in the definition of the field on page 64. In the proof below, we set $v_1 = a_1 + b_1\sqrt{p}$, $v_2 = a_2 + b_2\sqrt{p}$ and $v_3 = a_3 + b_3\sqrt{p}$, where $a_i \in Q$, $b_i \in Q$ for $i = 1, 2, 3$.

F1.

$$v_1 + v_2 \in (a_1 + a_2) + (b_1 + b_2)\sqrt{p} \in Q[\sqrt{p}],$$

and

$$v_1 \times v_2 = (a_1a_2 + pb_1b_2) + \sqrt{p}(a_1b_2 + a_2b_1) \in Q[\sqrt{p}].$$

F2.

$$(v_1 + v_2) + v_3 = (a_1 + a_2 + a_3) + \sqrt{p}(b_1 + b_2 + b_3);$$

and

$$v_1 + (v_2 + v_3) = (a_1 + a_2 + a_3) + \sqrt{p}(b_1 + b_2 + b_3),$$

So

$$(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3).$$

On the other hand

$$(v_1\times v_2)\times v_3 = a_1a_2a_3+pb_1b_2a_3+pa_1b_2b_3+pa_2b_1b_3+\sqrt{p}(a_1a_2b_3+pb_1b_2b_3+a_1b_2a_3+a_2b_1a_3).$$

and

$$v_1\times(v_2\times v_3) = a_1a_2a_3+pb_1b_2a_3+pa_1b_2b_3+pa_2b_1b_3+\sqrt{p}(a_1a_2b_3+pb_1b_2b_3+a_1b_2a_3+a_2b_1a_3).$$

So

$$(v_1 \times v_2) \times v_3 = v_1 \times (v_2 \times v_3).$$

F3.

$$v_1 + v_2 \in (a_1 + a_2) + (b_1 + b_2)\sqrt{p}; v_2 + v_1 = (a_2 + a_1) + (b_1 + b_2)\sqrt{p}.$$

So

$$v_1 + v_2 = v_2 + v_1.$$

On the other hand,

$$v_1 \times v_2 = (a_1 a_2 + p b_1 b_2) + \sqrt{p}(a_1 b_2 + a_2 b_1).$$

and

$$v_2 \times v_1 = (a_1 a_2 + p b_1 b_2) + \sqrt{p}(a_1 b_2 + a_2 b_1).$$

So

$$v_1 \times v_2 = v_2 \times v_1.$$

F4.

$$\begin{aligned} v_1 \times (v_2 + v_3) &= (a_1 + b_1\sqrt{p}) \times (a_2 + a_3 + \sqrt{p}(b_2 + b_3)) \\ &= a_1 a_2 + a_1 a_3 + p b_1 b_2 + p b_1 b_3 + \sqrt{p}(a_2 b_1 + a_3 b_1 + a_1 b_2 + a_1 b_3). \end{aligned}$$

On the other hand,

$$v_1 \times v_2 + v_1 \times v_3 = a_1 a_2 + a_1 a_3 + p b_1 b_2 + p b_1 b_3 + \sqrt{p}(a_2 b_1 + a_3 b_1 + a_1 b_2 + a_1 b_3).$$

F5.

$$\begin{aligned} 0 &:= 0 + 0\sqrt{p} \in Q[\sqrt{p}], \text{ for this element, } v + 0 = v. \\ 1 &:= 1 + 0\sqrt{p} \in Q[\sqrt{p}], \text{ for this element, } v \times 1 = v. \end{aligned}$$

F6. Given $v_1 \in Q[\sqrt{p}]$,

$$-v_1 = (-a_1) + (-b_1)\sqrt{p}.$$

Then we can verify that

$$v_1 + (-v_1) = 0.$$

F7. Given $v = a + b\sqrt{p} \in Q[\sqrt{p}]$ with $a, b \in Q$ and $v \neq 0$. Note that the condition $v \neq 0$ will give $a \neq 0$ or $b \neq 0$; otherwise $v = 0$. So we also have

$$a - b\sqrt{p} \neq 0.$$

We compute that

$$\frac{1}{a + b\sqrt{p}} = \frac{a - b\sqrt{p}}{(a + b\sqrt{p})(a - b\sqrt{p})} = \frac{a - b\sqrt{p}}{a^2 - pb^2} = \frac{a}{a^2 - pb^2} - \frac{b}{a^2 - pb^2}\sqrt{p},$$

which is the inverse of v because both $\dfrac{a}{a^2 - pb^2}$ and $-\dfrac{b}{a^2 - pb^2}$ are rational numbers.

That $Q[\sqrt{p}]$ is an order field follows from the fact that the real numbers $\mathbb{R}$ is an ordered field, and $Q[\sqrt{p}] \subset \mathbb{R}$. $\square$

8. P76 Ex. 7.

Proof. **Proof of a).** Define the set

$$S := \{u \in \mathbb{R} : (-\infty, u) \subset M\}.$$

The set S is not an empty set by the condition. Secondly S must be bounded above; otherwise if $(-\infty, u) \subset M$ for any $u \in \mathbb{R}$, then for any $x \in \mathbb{R}$, since $x \in (-\infty, x+1)$ and $(-\infty, x+1) \subset M$, we have $x \in M$. This implies that $\mathbb{R} \subset M$, which contradicts to that $M \neq R$. So S is bounded above. By the completeness axiom, there exists $U \in \mathbb{R}$, the least upper bound of S. We show that $(-\infty, U) \subset M$: for any $x \in (-\infty, U)$, $x < U$. So for $\varepsilon = U - x$, there exists $u \in S$ such that

$$u > U - (U - x) = x.$$

In others' words, $x \in (-\infty, u)$. $u \in S$ implies that $(-\infty, u) \subset M$. So $x \in M$. Hence

$$(-\infty, U) \subset M.$$

Proof of b). If $(-\infty, r) \subset M$, then by definition of S, $r \in S$. Of course $r \leq U$ because U is an upper bound of S. □

9. P76 Ex. 8.

Proof. When $a > 0$, the set is unbounded above. When $a < 0$, the set is unbounded below. We only prove the former claim. The proof for the second follows similarly.

When $a > 0$ and given any $M > 0$, by Theorem 6.3.2, there always exists an integer N such that

$$N \geq \frac{M - b}{a}.$$

that is to say

$$aN + b \geq M.$$

This proves the set $\{an + b : a > 0\}$ is unbounded above. □

Department of Mathematics, KU, Lawrence, KS 66045

E-mail address: `slshao@math.ku.edu`