

1. (not graded)– 1.7. Let $P(n)$ be the proposition that $7^n - 6n - 1$ is divisible by 36. Then $P(1)$ is the proposition that $7^1 - 6 \cdot 1 - 1 = 0$ is divisible by 36, which is immediate. To prove this proposition by induction, we now need only show that if $P(n)$ is true, then $P(n + 1)$ is true. So, to be precise, assume that $7^n - 6n - 1 = 36m$ for some integer m . Then a little algebra – noted in the hint in the back – and the use of the induction hypothesis shows that

$$7^{n+1} - 6(n+1) - 1 = 7(7^n - 6n - 1) + 36n = 36(7m + n).$$

That is, if $P(n)$ is true, then $P(n+1)$ is true. Thus the claim is established by Mathematical Induction.

2. – 2.4. Let $u = (5 - \sqrt{3})^{1/3}$. Then

$$u^3 = 5 - \sqrt{3} \implies (u^3 - 5)^2 = (-\sqrt{3})^2 = 3 \implies u^6 - 10u^3 + 22 = 0.$$

There are several ways to go from here. If $u \in \mathbf{Q}$, then $u^3 - 5 \in \mathbf{Q}$, hence $-\sqrt{3} \in \mathbf{Q}$, which we know to be impossible. Or, you can appeal to the Rational Zeros Theorem. If $u = \frac{p}{q}$ were rational and in lowest terms, then we would have $q \mid 1$ and $p \mid 22$, so $u \in \{\pm 1, \pm 2, \pm 11, \pm 22\}$. This is clearly impossible. (Numerically, $\sqrt{3} \approx 1.7$, so $5 - \sqrt{3} \approx 3.3$, so $1 < u < 2$.) I suspect you might have found some other ways to do it.

3. – 3.4. To prove in \mathbf{R} (using the axioms given on p. 13): (v) “ $0 < 1$ ” and (vii) “if $0 < a < b$, then $0 < b^{-1} < a^{-1}$ ”.

To prove (v), we observe following the hint that $1 \cdot 1 = 1$ by M3, with $a = 1$. Thus $1 = 1^2$, and so by (iv), $0 \leq 1$, hence either $0 < 1$ or $0 = 1$. How do we know that the second case does not occur?

Observe that if $0 = 1$, then for any $a \in F$, $0 \cdot a = 0$ (Thm 3.1(ii)) and $1 \cdot a = a$ (M3). It thus follows that $a = 0$ for every $a \in F$! In fact, one can define a field consisting of a single element $\{0\}$ and so that $0 + 0 = 0 \cdot 0 = 0$. This satisfies the axioms in a singularly uninteresting way. (Axiom M4 is void, because there is no $a \neq 0$.) Usually, this material is presented a little more carefully in print, so that $0 \neq 1$ as part of the expression of M3. Nonetheless, this problem asks about \mathbf{R} , and it's apparent that $0 \neq 1$ for the reals, since $\mathbf{N} \subset \mathbf{R}$.

In (vii), we are given $0 < a < b$, so that a^{-1} and b^{-1} are both defined. By O1, these elements can be compared to each other. Note from the definition of the ordering that either $x \leq y$ or $y < x$ for any two real numbers. But

$$\begin{aligned} a^{-1} \leq b^{-1} &\implies a \cdot a^{-1} \leq a \cdot b^{-1} \implies 1 \leq a \cdot b^{-1} \\ \implies b = 1 \cdot b &\leq (a \cdot b^{-1}) \cdot b = a \cdot (b^{-1} \cdot b) = a \cdot 1 = a; \quad \text{that is, } b \leq a. \end{aligned}$$

And we know that $a < b$, so that $b \leq a$ is impossible. Thus, it is not true that $a^{-1} \leq b^{-1}$, and we are forced to conclude that $b^{-1} < a^{-1}$.

4. – 4.6. Let S be a non-empty bounded subset of \mathbf{R} . (Note: “bounded” means bounded above and bounded below, and by the Completeness Axiom, this means that $\sup S$ and $\inf S$ are defined.)

(a) Prove that $\inf S \leq \sup S$. Well, suppose $x \in S$, which you can assume is possible because S is non-empty. By the definition of \sup and \inf , we know that $\inf S \leq x$ and $x \leq \sup S$, so putting this together by O3, we get $\inf S \leq \sup S$. Note the mysterious role of x in this problem: it is both essential and completely unimportant!

(b) Suppose $\inf S = \sup S$. Then we can continue the inequality above to $\inf S \leq x \leq \sup S \leq \inf S$. Thus, if $x \in S$, then $\inf S \leq x$ and $x \leq \inf S$, so by O2, $x = \inf S = \sup S$. That is, S contains exactly one element, x .

5. (not graded) 4.9. Done in the back of the book.

6. 4.14. Suppose A and B are bounded subsets of \mathbf{R} and

$$A + B = \{a + b : a \in A, b \in B\}.$$

(a) We wish to show that $\sup A + \sup B = \sup(A + B)$. To shorten notation, let $S_A = \sup A$ and $S_B = \sup B$. If $x \in A + B$, then $x = a + b$ for some $a \in A, b \in B$. It follows that $a \leq S_A$ and $b \leq S_B$, so adding, $x = a + b \leq S_A + S_B$. Thus, $S_A + S_B$ is an upper bound for $A + B$. We have to prove that it is a supremum; that is, a *least* upper bound. Suppose $M < S_A + S_B$. We want to show that M is *not* an upper bound for $A + B$. Let $r = S_A + S_B - M > 0$. By hypothesis, $S_A - r/2$ is not an upper bound for A and $S_B - r/2$ is not an upper bound for B , because these are smaller than the respective suprema. This means that there exist $a \in A$ and $b \in B$ so that $a > S_A - r/2$ and $b > S_B - r/2$. The sum of these two elements is in $A + B$ and

$$a + b > (S_A - r/2) + (S_B - r/2) = S_A + S_B - r = M$$

This means that M is *not* a supremum for $A + B$, which verifies the claim that $S_A + S_B$ is the **least** upper bound.

(b) Since $(-A) + (-B) = -(A + B)$ by definition, part (a) and the argument of Theorem 4.5 (i.e., $\inf S = -\sup(-S)$) imply that

$$\begin{aligned} \sup(-A) + \sup(-B) &= \sup(-(A + B)) \implies (-\inf A) + (-\inf B) = -\inf(A + B) \\ &\implies \inf A + \inf B = \inf(A + B). \end{aligned}$$

7. – 5.2. (a) Let $S_1 = \{x : x < 0\}$. This is the set of all negative real numbers. It can be written in interval form as $(-\infty, 0)$, which tells us that $\inf S_1 = -\infty$ (it is not bounded below) and $\sup S_1 = 0$.

(b) Let $S_2 = \{x : x^3 \leq 8\}$. Presumably, you know from calculus that the function $f(x) = x^3$ is increasing, so $S_2 = (-\infty, 8^{1/3}]$. Here, $8^{1/3} = 2$, and we see that $\inf S_2 = -\infty$ (it is not bounded below) and $\sup S_2 = 2$.

(c) Let $S_3 = \{x^2 : x \in \mathbf{R}\}$. We know that $0 \leq x^2$ for every real x ; conversely, if $y > 0$, then $y = (\sqrt{y})^2$. Thus, $S_3 = [0, \infty)$, and $\inf S_3 = 0$ and $\sup S_3 = \infty$ (it is not bounded above.)

(d) Let $S_4 = \{x : x^2 < 8\}$. Again, we have to rely on calculus to recognize that $S_4 = (-\sqrt{8}, \sqrt{8})$. This is, finally, a bounded set, with $\inf S_4 = -\sqrt{8}$ and $\sup S_4 = \sqrt{8}$.

8a. Let $A = \{n + 5/n : n \in \mathbf{N}\}$. Compute $\inf A$.

It makes sense to let $f(n) = n + 5/n$ and compute some values of f : we have $f(1) = 6, f(2) = 9/2, f(3) = 14/3, f(4) = 21/4, f(5) = 6$. The hint suggests that we look at $f(x) = x + 5/x$ as a real function. The derivative is $f'(x) = 1 - 5/x^2$. Thus, if $x^2 < 5$, then f is decreasing, and if $x^2 > 5$, then f is increasing. That is, if $a < b < \sqrt{5} < c < d$, then $f(a) > f(b)$ and $f(c) < f(d)$. As applied here, $f(1) > f(2)$ and $f(3) < f(4) < f(5) < \dots$. Thus, the smaller of $f(2)$ and $f(3)$ will be a lower bound, and clearly the greatest lower bound. Since $f(2) = 4.5$ and $f(3) \approx 4.67$, $\inf A = 4.5$. Alternatively, one can calculate $f(1), f(2), f(3), f(4)$ and then observe that if $n \geq 5$, then $n + 5/n \geq 5 > 4.5$.

I don't know why I asked (b), but the same argument applies, with $g(n) = n + 6/n$. As a real function, g' changes sign at $\sqrt{6}$, which is also in $(2, 3)$. It follows that the infimum of $\{g(n)\}$ occurs at either $n = 2$ or $n = 3$. In this case, $g(2) = g(3) = 5$ is the infimum.

9. Prove that there are no ordered finite fields.

Well, there's a small glitch here. If you let F be the field consisting of the single element 0, then as noted above, the resulting field is well-defined and trivially ordered, since $0 \leq 0$. Leaving this aside, we have $0 < 1$ as above. This means that $0 + 1 < 1 + 1$, so $0 < 1 < 1 + 1$. Continuing in this way, we obtain an infinite chain of elements, each one of which is larger than the previous one:

$$0 < 1 < 1 + 1 < 1 + 1 + 1 < 1 + 1 + 1 + 1 < \dots$$

This is a contradiction in a finite field.

Small technical point: in a finite field, the element "1" may not be the same as the integer "1", so "1+1" needn't equal 2. (In the example I gave in class on the finite field F_2 with two elements, $1 + 1 = 0$!)

10. Suppose $a, b \in \mathbf{N}$, and $\sqrt{a}, \sqrt{b} \notin \mathbf{N}$, and let $\alpha = \sqrt{a} + \sqrt{b}$.

(a) Prove that α is an algebraic integer by finding a monic polynomial f with integer coefficients so that $f(\alpha) = 0$. Well,

$$\begin{aligned} (\alpha - \sqrt{a})^2 &= \alpha^2 - 2\sqrt{a} \cdot \alpha + a = b \implies \alpha^2 + a - b = 2\sqrt{a} \cdot \alpha \\ &\implies \alpha^4 + 2(a - b)\alpha^2 + (a - b)^2 = 4a \cdot \alpha^2, \end{aligned}$$

so $f(x) = x^4 - 2(a + b)x^2 + (a - b)^2$ will do the trick.

(b) Prove that α is irrational by deriving a contradiction from the equation $\sqrt{a} + \sqrt{b} = m$ for an integer m .

Since α is an algebraic integer, we know that if it is rational, it is an integer, and by its definition, a positive one at that. Given the equation above, we have

$$\sqrt{b} = m - \sqrt{a} \implies b = m^2 + a - 2m\sqrt{a} \implies \sqrt{a} = \frac{m^2 + a - b}{2m} \in \mathbf{Q}$$

As previously noted in class, if a is an integer and \sqrt{a} is rational, then $\sqrt{a} \in \mathbf{Z}$. This is a contradiction to the hypotheses of the problem.