1. Let \( y = 0 \cdot x \).
\[ 0 \cdot x = (0 + 0) \cdot x \text{ (zero is the neutral element for \( \cdot \))} \]
\[ = 0 \cdot x + 0 \cdot x \text{ (distributivity)} \]
Then \( y = y + y \). Adding \(-y\) we have \((-y) + y = (y + y) = ((-y) + y) + y\) (associativity) implies \(0 = y\).

(f) Suppose there exist two inverses \( x' \) and \( x'' \) of \( x \) relative to \(+\). Then \( x' + x = x + x' = 0 \) and \( x'' + x = x + x'' = 0 \).
Add \( x'' \) to the first relation.
\[ x'' + (x + x') = x'' + 0 = x'' \text{ (neutral element)} \]
But left hand side is equal to \( (x'' + x) + x' = 0 + x' = x' \) by associativity. We have \( x' = x'' \).

(b) Because \((-x)\) is the notation for the unique element \( x' \) such that \( x' + x = x + x' = 0 \), this same relation shows that by changing roles, \( x \) must be the inverse of \((-x)\) relative to \(+\). That means \(-(-x) = x\).

(a) \(0 = 0 \cdot x = ((-1) + 1) \cdot x = (-1) \cdot x + 1 \cdot x = (-1) \cdot x + x\). This implies that \((-1) \cdot x\) satisfies the property defining the element \((-x)\). That element is unique, thus we are done.

(c) Is a consequence of (b).

(e) If \( x > y \) then we may add the number \( z = (-y) + (-x) \) on both sides and the equality is preserved. Then \(-y > -x\).

2. \( a \cdot x + b = c \)
\[ (a \cdot x + b) + (-b) = c + (-b) \]
\[ a \cdot x + (b + (-b)) = c + (-b) \]
\[ a \cdot x + 0 = c + (-b) \]
\[ a \cdot x = c + (-b) \]
If \( a \neq 0 \) then \( a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (c + (-b)) \)
\[ (a^{-1} \cdot a) \cdot x = a^{-1} \cdot (c + (-b)) \]
\[ 1 \cdot x = a^{-1} \cdot (c + (-b)) \]
\[ x = a^{-1} \cdot (c + (-b)) \]
which can be written \( x = \frac{c-b}{a} \).
If \( a = 0 \) then the equation has no solution if \( b \neq c \) and has solution all real numbers if \( b = c \).

6. We want to show that \( \mathbb{Q}[\sqrt{2}] \) is a closed set for all required operations. For any \( x = p' + q' \sqrt{2} \) and \( y = p'' + q'' \sqrt{2} \) in \( \mathbb{Q}[\sqrt{2}] \), \( p', q', p'', q'' \in \mathbb{Q} \).

- \( x + y \in \mathbb{Q}[\sqrt{2}] \), i.e. there exist \( p, q \in \mathbb{Q} \) such that \( x + y = p + q \sqrt{2} \).
  \[ x + y = (p' + p'') + (q' + q'' \sqrt{2}) = p + q \sqrt{2} \in \mathbb{Q}[\sqrt{2}] \because p = p' + q' \quad \text{and} \quad q = q' + q'' \quad \text{are in \( \mathbb{Q} \).} \]
\[ x \in \mathbb{Q}[\sqrt{2}] \]
\[ x = (-p') + (-q')\sqrt{2} \]
\[ xy \in \mathbb{Q}[\sqrt{2}] \]
\[ xy = (p'p'' + 2q'q'') + (p'q'' + p''q')\sqrt{2} \]
\[ x^{-1} \in \mathbb{Q}[\sqrt{2}], \text{ when } x \neq 0, \]
\[ x^{-1} = \frac{p'}{(p'p'')^2 + 2(q'q'')^2}\sqrt{2} \]

after rationalization, i.e. multiplication by \( p' - q'\sqrt{2} \) at both numerator and denominator.

If we have shown closure, then all eleven axioms of a commutative field are automatically satisfied because \( \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R} \).

8.

Remark. There is only one solution \( v > 0 \) to \( v^n = c, c > 0, n \in \mathbb{N}^* \).

Let \( w > 0 \) be another solution. Since
\[ v^n - w^n = (v - w)(v^{n-1} + v^{n-2}w + \ldots + vw^{n-2} + w^{n-1}) \]
and the second factor is strictly positive, \( v^n = w^n = c \) implies \( v = w \), which proves uniqueness.

From now on \( v \) will be denoted by \( \sqrt[n]{c} = c^{\frac{1}{n}} \), the \( n \)-th root of \( c \).

In the exercise, \( n \) is \( y \).

To prove that \( (a^{\frac{1}{n}})^n = (a^y)^{\frac{1}{n}} \) we only need to show that

"The number \( v \), the \( y \)-th root of \( a \), raised to power \( x \), equals the number \( w \), the \( y \)-th root of \( a^x \)."

If the two are equal, then we are justified to denote their common value by \( a^{\frac{x}{y}} \).

By definition, \( v > 0, v^y = a \) and \( w > 0, w^y = a^x \). Then
\[ v^x = w \]
if and only if \( (v^x)^y = w^y \) from the remark proved above. Notice that
\[ (v^x)^y = v^{xy} = (v^y)^x = a^{xy} = w^y \]
so we are done.

It is important to note that we were allowed to manipulate the exponents because they were natural numbers and \( v^n = v \cdot v \cdot \ldots \) \( v \) times, the product of \( v \) with itself \( n \) times, \( \forall v \in \mathbb{N}^* \). What this exercise achieved, is to allow us to do the same for rational exponents as well.

9. For \( x = (p', q') \) and \( y = (p'', q'') \) we have \( x \leq y \) if either \( x < y \) or \( x = y \). In other words,

\[ x \leq y \text{ equivalent to } \]

Either (1) \( p' < p'' \); or (2) \( p' = p'' \) and \( q' \leq q'' \).

We shall verify the three axioms of an ordered set.

- (i) \( x \leq y \) evident with (2) and \( q' = q'' \).
- (ii) \( x \leq y \text{ and } y \leq x \), then \( x = y \).
  
  Suppose \( p' < p'' \). Then \( y \leq x \) is false. Suppose \( p'' < p' \). Then \( x \leq y \) is false. Assuming both \( x \leq y \) and \( y \leq x \), the only remaining possibility is \( p' = p'' \). If \( p' = p'' \), we are in case (2) and \( x \leq y \) implies \( q' \leq q'' \); meanwhile \( y \leq x \) implies \( q'' \leq q' \). Thus \( q' = q'' \). Both coordinates are equal, we then have \( x = y \).
- (iii) \( x \leq y \text{ and } y \leq z \), then \( x \leq z \). Denote \( z = (p'''', q'''') \). First notice that if \( x \leq y \) then \( p' \leq p'' \), since the case \( p' > p'' \) contradicts both (1) and (2). Repeat this observation for \( y \leq z \) to conclude that \( p'' \leq p''' \). By transitivity of the usual order relation on the real numbers, \( p' \leq p''' \). We are not done yet. Suppose \( p' < p''' \); then \( x < z \) and we are done being in
case (1). If \( p' = p'' \), necessarily \( p' = p''' = p'''' \) and we are in case (2) for both inequalities. But then \( q' \leq q'' \leq q''' \) which implies that \( p' = p'''' \) and \( q' \leq q''' \), which is case (2).

- We can prove more: Any two \( x, y \) are comparable. Pick two pairs. The first components \( p', p'' \) are real numbers, and exactly one of \( p' < p'', p' > p'' \) or \( p' = p'' \) is true. If one of the first two is true, then we are in case (1), and \( x < y \), respectively \( x > y \). If the third case is true, then we are in (2), \( q', q'' \) are real numbers and exactly one of \( q' < q'', q' > q'' \) or \( q' = q'' \) is true, corresponding to \( x < y, x > y, x = y \), respectively. In all cases we were able to compare \( x \) with \( y \).

4[T].

This proof is identical to the case \( p = 2 \), and was done in class.

Suppose \( p = \left( \frac{m}{n} \right)^2 \), with \( m, n \in \mathbb{N}, n \neq 0 \), an irreducible fraction, i.e. there exists no prime that divides both \( m \) and \( n \). If a fraction is not irreducible, it can be simplified by the greatest common divisor of \( m \) and \( n \) and it becomes irreducible. Then \( pn^2 = m^2 \). This implies that \( p \) divides \( m^2 \). There is no way that \( p \) divides \( m^2 \) without dividing \( m \) (the factor \( p \) either is or is not in the factorization of \( m \)). We then have a number \( m_1 \in \mathbb{N} \) such that \( m = pm_1 \). Re-write the equality as \( pm^2 = p^2m_1^2 \), divide by \( p \), to obtain \( pm_1^2 = n^2 \). In new roles, the numbers \( m_1 \) and \( n \) allow us to apply the same reasoning to see that \( p \) divides \( n \) as well. This is a contradiction, since \( m \) and \( n \) have no common prime factors. The solution \( v \) of \( v^2 = p \) (that is, \( v = \sqrt{p} \)), cannot be written as the ratio of two integers, hence is not a rational number.

5[T].

- (a) \( S \) contains
  - (1) numbers of the form \(-\frac{1}{n}, n \geq 1 \) odd and
  - (2) numbers numbers of the form \(-\frac{1}{n} + 2n^2, n \geq 2, n \) even.

  Since \( 2n^2 - \frac{1}{n} \geq n \), the set does not have an upper bound, and the supremum is not a real number. We can say this by writing \( \sup S = +\infty \).

  Since \( 2n^2 - \frac{1}{n} \geq n \geq 2 \) and the odd number sequence is increasing in \( n \), the infimum is reached for the odd number \( n = 1 \) and so \( \inf S = -1 \).

- (b) \( S = (-3, 3) \). \( \inf S = -3, \sup S = +3, \) max and min do not exist.

- (c) \( S = [-\sqrt{7}, \sqrt{7}] \). \( \inf S = -\sqrt{7} = \min S, \sup S = +\sqrt{7} = \max S \).

- (d) The inequality is equivalent to \( -5 < 2x + 1 < 5 \) so \( S = (-3, 2) \). \( \inf S = -3, \sup S = +2, \) max and min do not exist.

- (e) \( S = (-1, 1) \). \( \inf S = -1, \sup S = +1, \) max and min do not exist.

- (f) \( S = [-\sqrt{7}, \sqrt{7}] \cap \mathbb{Q} \). \( \inf S = -\sqrt{7}, \sup S = +\sqrt{7}, \) max and min do not exist.

7[T].
(a) Let \( x \in S \) (it exists since \( S \) is not empty). Then \( \sup S \) is an upper bound of \( S \), i.e. \( x \leq \sup S \). Similarly, \( \inf S \) is a lower bound of \( S \), i.e. \( \inf S \leq x \). Then \( \inf S \leq x \leq \sup S \).

Conditions for equality. If \( \inf S = \sup S = s \), then for any \( x \in S \) we must have \( s \leq x \leq s \), implying \( x = s \). The only case when this can happen is when \( S = \{ s \} \), \( s \in \mathbb{R} \), i.e. \( S \) has exactly one element.

10[T].
(a) Pick any element of \( x \in S + T \). That means, there exist \( s \in S \) and \( t \in T \) such that \( x = s + t \). Since \( s \leq \sup S \) and \( t \leq \sup T \), we immediately have \( x = s + t \leq \sup S + \sup T \). We have shown that \( \sup S + \sup T \) is an upper bound of \( S + T \).

To show that it is the supremum (least upper bound), we pick \( \epsilon > 0 \). We want to show that there exists \( x_0 \in S + T \) such that \( x_0 > \sup S + \sup T - \epsilon \). But we know that \( \sup S \) has the property that for an error we deliberately choose equal to \( \epsilon/2 \), there exists \( s_0 \in S \) such that \( s_0 > \sup S - \epsilon/2 \). Similarly, there exists \( t_0 \in T \) such that \( t_0 > \sup T - \epsilon/2 \). It follows that for the choice \( x_0 = s_0 + t_0 \) we have \( x_0 > \sup S + \sup T - \epsilon \) and we are done.

The proof for \( \inf \) is the same.

11[T].
We can do problem 11 directly, but we shall prove a useful result:
\[ \sup(-S) = -\inf S \]
for any \( S \) bounded above and below. Here \( -S = \{ -s \mid s \in S \} \).

Read the remarks at the end to see that the statement is true for any \( S \subseteq \mathbb{R} \) with the appropriate conventions on \( \pm \infty \).

We first prove that \( -\inf S \) is an upper bound of \( -S \). Since \( \inf S \leq s, \forall s \in S \), we have \( -s \leq -\inf S \).

We want to show that if \( M \) is an upper bound of \( -S \), then \( M \geq -\inf S \). If we know that \( -s \leq M, \forall s \in S \), then \( s \geq -M \) and then \( -M \) is a lower bound of \( S \). This implies that \( -M \leq \inf S \), or equivalently, \( M \geq -\inf S \).

The rest of problem 11 is an application of problem 10.

Remark on part (b) of 10, 11.
A set \( S \) is said bounded when it is bounded both above and below.

When a set is either unbounded below or unbounded above, we say it is unbounded.

When a set \( S \) does not have an upper bound, we say it is unbounded above, and write \( \sup S = +\infty \).

When a set \( S \) does not have a lower bound, we say it is unbounded below, and write \( \inf S = -\infty \).

All relations in problems 10, 11 are true with the obvious modifications of the calculus with \( \pm \infty \).