Math 295. Solutions for Homework 1

“A police corporal was suspended and ordered to undergo psychiatric evaluation because he writes the number seven with a line through the down stroke. Brian Yinger said he tried to break the habit when he was ordered to six months ago but was brought before a department disciplinary board when he forgot while writing some reports. … He said he fears the incident might hurt his career and cost him a promotion to sergeant. Yinger said he was considering a civil lawsuit. The dispute could end up costing the city nearly $4,000 in transcripts, arbitration fees and back pay, officials said.”


(1) Let \( S \) be a set. Recall that \( \mathcal{P}(S) \) denotes the power set of \( S \), that is, the set of all subsets of \( S \). Define a binary operation \( \star \) on \( \mathcal{P}(S) \) by

\[
A \star B = \begin{cases} 
A \cup B & \text{provided that } A \cap B = \emptyset \\
S & \text{provided that } A \cap B \neq \emptyset 
\end{cases}
\]

for subsets \( A \) and \( B \) of \( S \).

(a) Show that \( \star \) is an associative, commutative binary operation on \( \mathcal{P}(S) \). (Note, this is mostly an exercise in “being careful”.)

(b) Is there a \( \star \)-identity? (Answering “yes” or “no” will get you zero points on such questions. You must both answer the question and justify your answer.)

(c) If the answer to the above question was “yes”, then how many elements of \( \mathcal{P}(S) \) have \( \star \)-inverses?

(a): Suppose \( A \) and \( B \) are subsets of \( S \). Since exactly one of \( A \cap B = \emptyset \) or \( A \cap B \neq \emptyset \) is true, the assignment \( (A, B) \mapsto A \star B \) defines a function

\[
\star : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S).
\]

Hence, \( \star \) is a binary operation on \( \mathcal{P}(S) \).

Since \( A \cup B = B \cup A \) and \( A \cap B = B \cap A \) for all elements \( A, B \in \mathcal{P}(S) \), we have: if \( A \cap B = \emptyset \), then \( B \cap A = \emptyset \) and so \( A \star B = A \cup B = B \cup A = B \star A \); if \( A \cap B \neq \emptyset \), then \( B \cap A \neq \emptyset \) and so \( A \star B = S = B \star A \). Hence \( \star \) is commutative.

Finally, we show that \( \star \) is associative. Let \( A, B, C \) be subsets of \( S \). We consider two cases:

Case I: Suppose that \( A, B, \) and \( C \) are mutually disjoint subsets of \( S \) (that is, \( A \cap B = \emptyset, B \cap C = \emptyset, \) and \( A \cap C = \emptyset \)). In this case, we have \( (A \cup B) \cap C = \emptyset \) and \( A \cap (B \cup C) = \emptyset \). Thus,

\[
(A \star B) \star C = (A \cup B) \star C = (A \cup B) \cup C
\]

and

\[
A \star (B \star C) = A \star (B \cup C) = A \cup (B \cup C).
\]

Thus, since taking unions is associative, we have \( (A \star B) \star C = A \star (B \star C) \).

Case II: Suppose that at least one of \( A \cap B, A \cap C, \) or \( B \cap C \) is nonempty. We claim that both \( A \star (B \star C) \) and \( (A \star B) \star C \) are equal to \( S \).

We begin by looking at \( A \star (B \star C) \). If \( B \cap C \neq \emptyset \), then \( A \star (B \star C) = A \star S = S \). If \( B \cap C = \emptyset \), then at least one of \( A \cap B \) or \( A \cap C \) is nonempty. In either case, we have \( A \cap (B \cup C) \neq \emptyset \). Thus, if \( B \cap C = \emptyset \), then

\[
A \star (B \star C) = A \star (B \cup C) = S.
\]

We now examine \( (A \star B) \star C \). If \( A \cap B = \emptyset \), then \( (A \star B) \star C = S \star C = S \). If \( A \cap B \neq \emptyset \), then at least one of \( A \cap C \) or \( B \cap C \) must be nonempty. In either case, we have \( (A \cup B) \cap C \neq \emptyset \). Thus, if \( A \cap B = \emptyset \), then

\[
A \star B \star C = (A \cup B) \star C = S.
\]

(b): Yes. The empty set is a \( \star \)-identity. Since, for all \( A \in \mathcal{P}(A) \), we have \( A \cap \emptyset = \emptyset \cap A = \emptyset \), it follows that \( A \star \emptyset = A = \emptyset \star A \).
(c) Exactly one: the identity itself. Suppose $A$ is a subset of $S$ and $A'$ is a $\ast$-inverse of $A$. By definition of $\ast$-inverse, we must have

$$A \ast A' = A' \ast A = \emptyset.$$  

However, by the definition of $\ast$, we also have $A \subseteq A \ast A' = \emptyset$. Thus, the only subset of $S$ that can have a $\ast$-inverse is the empty set. Since $\emptyset \ast \emptyset = \emptyset$, the empty set is its own $\ast$-inverse.

(2) Suppose $(F, P)$ is an ordered field. Suppose $a, b, c \in F$ with $a \geq 0$ and $b \geq 0$.

(a) Show that $c \in P$ if and only if $c^{-1} \in P$.

(b) Show that $a = b$ if and only if $a^2 = b^2$. (Note, if $b = 0$, then we have $a = 0$ if and only if $a^2 = 0$.)

(c) Show that $a > 0$ if and only if $a^2 > 0$.

(d) For $b > 0$, show that $a > b$ if and only if $a^2 > b^2$.

(e) Use the above to conclude:

$$a > b \text{ if and only if } a^2 > b^2$$

and

$$a = b \text{ if and only if } a^2 = b^2.$$  

We have already used this fact in class.

(a) We first show that if $c \in P$, then $c^{-1} \in P$. Since $c \in P$, we have $c \neq 0$ and so $c^{-1}$ exists. Since $c \cdot c^{-1} = 1 \neq 0$, we conclude that $c^{-1} \neq 0$. Thus, by trichotomy, we have either $c^{-1} \in P$ or $-c^{-1} \in P$, but not both. If $c^{-1} \in P$, then we are done. So, suppose that $-c^{-1} \in P$. Since $P$ is closed under multiplication, we must then have $c \cdot (-c^{-1}) \in P$. However, from class, we know $c \cdot (-c^{-1}) = -c^{-1} = -1 \notin P$. This is a contradiction.

We now show that if $c^{-1} \in P$, then $c \in P$. Implicit in this statement is the assumption: $c \neq 0$ (If $c = 0$, then we cannot speak of $c^{-1}$.) Since $c^{-1} \in P$, from the previous paragraph, we know $(c^{-1})^{-1} \in P$. But, from class, we know that $(c^{-1})^{-1} = c$.

(b): We first show that if $a = b$, then $a^2 = b^2$. We have

$$a^2 = a \cdot a = a \cdot b = b \cdot b = b^2.$$  

Now suppose that $a^2 = b^2$. Note that

$$(b - a)(b + a) = (b - a)b + (b - a)a = (bb - ab) + (ba - aa)$$

$$= ((b^2 - ab) + ba) - a^2 = (b^2 + (-ab + ba)) - a^2$$

$$= (b^2 + (-ab + ab)) - a^2 = (b^2 + 0) - a^2$$

$$= b^2 - a^2$$

Since $b^2 - a^2 = 0$, from Equation (??) and class we conclude that at least one of $(b - a)$ or $(b + a)$ is zero. If $(b - a) = 0$, then $b = a$ and we are finished. Suppose then that $b - a \neq 0$. In this case, we must have $b + a = 0$. Consequently, $b$ is the additive inverse of $a$. Since $b \geq 0$ and $a \geq 0$, from trichotomy we conclude that $a = b = 0$. (If $a \neq 0$, then, from the given, $a \in P$ and so $b = -a \not\in P$, violating the given information). But, if $a = b = 0$, then $b - a = 0$, a contradiction.

(c): Suppose first that $a > 0$. This means that $a \in P$ and so, since $P$ is closed with respect to multiplication, we must have $a^2 = aa \in P$. Thus $a^2 > 0$.

Now suppose that $a^2 > 0$. We already know that $a \geq 0$, so it is enough to show that $a \neq 0$. If $a = 0$, then $a^2 = aa = a0 = 0$. Thus, $a^2 > 0$ implies $a > 0$.

(d): Suppose $b > 0$.

We first show that if $a > b$, then $a^2 > b^2$. We need to show that $(a^2 - b^2) \in P$. Since $a > b$ and $b > 0$ we have (from class) $a > 0$. Thus, $a$, $b$, and $(a - b)$ belong to $P$. Since $P$ is closed with respect to addition, we have $a + b \in P$. Since $P$ is closed with respect to multiplication, we conclude that $(a - b)(a + b) \in P$. From Equation (??) this means $a^2 - b^2 \in P$, or $a^2 > b^2$.  

Suppose now that \( a^2 > b^2 \). Since \( b > 0 \), from part (c) we have \( b^2 > 0 \). Since \( a^2 > b^2 \) and \( b^2 > 0 \), we have (from class) \( a^2 > 0 \). Thus, from part (c) we have \( a > 0 \). We now know \( a, b, \) and \( a^2 - b^2 \) belong to \( P \). We want to conclude that \( a - b \in P \).

Since \( a, b \) belong to \( P \), we have \( (a + b) \in P \), and, thanks to part (a), we have \( (a + b)^{-1} \in P \). Thus
\[
(a - b) = (a - b)1 = (a - b)((a + b)(a + b)^{-1}) = [(a - b)(a + b)](a + b)^{-1}.
\]
From Equation (23), we conclude
\[
a - b = (a^2 - b^2)(a + b)^{-1}.
\]
Since \( P \) is closed under multiplication and both \( a^2 - b^2 \in P \) and \( (a + b)^{-1} \in P \), we conclude that \( a - b \in P \).

(e): We first show that
\[
a > b \text{ if and only if } a^2 > b^2.
\]
Since \( b \geq 0 \), we have \( b = 0 \) or \( b \in P \). If \( b = 0 \), then the statement follows from part (c). If \( b \in P \), then the statement follows from part (d).

The statement
\[
a = b \text{ if and only if } a^2 = b^2
\]
is part (b).

(3) The point of this problem is to show that there may be more than one way to order a field (that is, the choice of \( P \) is not necessarily uniquely determined). See page 572 for more discussion of this example. Define
\[
\mathbb{Q}(\sqrt{2}) := \{(a + b\sqrt{2}) \in \mathbb{R} \mid a, b \in \mathbb{Q}\}
\]

(a) Show that with respect to the usual binary operations of addition and multiplication in \( \mathbb{R} \), the set \( \mathbb{Q}(\sqrt{2}) \) is a field. Be very careful about how you justify the existence of multiplicative inverses.

(b) Suppose \( z = a + b\sqrt{2}, w = r + s\sqrt{2} \) are two elements of \( \mathbb{Q}(\sqrt{2}) \). Show that if \( z = w \), then \( a = r \) and \( b = s \).

(c) From the previous part of this problem, we can unambiguously define \( \overline{z} = a - b\sqrt{2} \). The operation \( w \mapsto \overline{w} \) on \( \mathbb{Q}(\sqrt{2}) \) is called conjugation. It has many wonderful properties; for example, show that

(i) \( \overline{z \cdot w} = \overline{z} \cdot \overline{w} \).

(ii) \( \overline{z} = z \) if and only if \( z \in \mathbb{Q} \).

(iii) Formulate and prove a statement describing how conjugation and addition interact.

(d) Define
\[
P := \{z \in \mathbb{Q}(\sqrt{2}) \mid \overline{z} > 0 \text{ in } \mathbb{R} \}.
\]

Show that \( (F, P) \) is an ordered field. Since \( -\sqrt{2} \in P \), this order is different from the standard order structure.

(a): Suppose \( a, b, r, s \in \mathbb{Q} \). Let \( w = r + s\sqrt{2} \) and \( z = a + b\sqrt{2} \). We first show that \( w + z \) and \( wz \) belong to \( \mathbb{Q}(\sqrt{2}) \). Well, by using the fact that \( \mathbb{R} \) is a field, we conclude:
\[
w + z = (r + c) + (s + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})
\]
and
\[
wz = (rc + 2bd) + (rd + sc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).
\]
Since \( \mathbb{Q}(\sqrt{2}) \) is closed under addition and multiplication and since it is a subset of \( \mathbb{R} \) (with the same operations!), properties (P1), (P4), (P5), (P8), and (P9) are free. For (P2) and (P3): The element \( 0 = 0 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \) is the additive identity, and the additive inverse of \( w \) is \( -w = -r - s\sqrt{2} \). For (P6): the element \( 1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \) is the multiplicative identity. If \( z \neq 0 \), then \( z^{-1} \) exists in \( \mathbb{R} \). To verify (P7) we need to know that \( z^{-1} \in \mathbb{Q}(\sqrt{2}) \).
Since \( z \neq 0 \), at least one of \( a \) or \( b \) is nonzero. Thus, since \( a \) and \( b \) are rational, we conclude that \( a \neq b\sqrt{2} \), or, in other words: \( a - b\sqrt{2} \neq 0 \). We calculate:

\[
\begin{align*}
z^{-1} &= (a + b\sqrt{2})^{-1} = (a + b\sqrt{2})^{-1} \cdot 1 = (a + b\sqrt{2})^{-1} \cdot [(a - b\sqrt{2})^{-1}(a - b\sqrt{2})] \\
&= [(a + b\sqrt{2})^{-1}(a - b\sqrt{2})^{-1}][a - b\sqrt{2}] \\
&= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})
\end{align*}
\]

(b) If \( z = w \), then \( (a - r) = (b - s)\sqrt{2} \). We either have that both sides are zero (in which case \( a = r \) and \( b = s \)) or both sides are nonzero. In the latter case, we conclude \( (b - s) \neq 0 \) and so

\[
\sqrt{2} = \frac{(a - r)}{(b - s)}.
\]

The right-hand-side of this equality is a rational number. However, from class we know that \( \sqrt{2} \) is not rational, a contradiction.

(ci): Recall from class that for elements \( c, d \) in a field we have \((-c)d = c(-d) = -cd \) and \( cd = (c)(-d) \). Moreover, since \(-c - d \) is an additive inverse of \( c + d \), we conclude from the uniqueness of additive inverses that \(-(c + d) = -c - d \).

We have

\[
\overline{z \cdot w} = (a + b\sqrt{2})(r + s\sqrt{2}) = (ar + 2bs) + (as + br)\sqrt{2}
\]

\[
= (ar + 2bs) - (as + br)\sqrt{2}.
\]

On the other hand,

\[
\overline{z \cdot w} = (a + (-b)\sqrt{2})(r + (-s)\sqrt{2}) = (ar + (-b)(-s)) + (a(-s) + (-b)r)\sqrt{2}
\]

\[
= (ar + bs) + (-as - br)\sqrt{2} = (ar + bs) - (as + br)\sqrt{2}
\]

(cii) If \( z = \overline{\omega} \), then \( a + b\sqrt{2} = a - b\sqrt{2} \). From part (b) we conclude that \( b = 0 \) and so \( z = a \in \mathbb{Q} \).

(ciii) The appropriate statement is:

\[
\overline{z + w} = \overline{z} + \overline{w}.
\]

We have

\[
\overline{z + w} = (a + r) + (b + s)\sqrt{2} = (a + r) - (b + s)\sqrt{2}
\]

and

\[
\overline{z + w} = (a - b\sqrt{2}) + (r - s\sqrt{2}) = (a + r) + (-b - s)\sqrt{2}.
\]

The result follows.

(d) We begin by showing that \( P \) is closed with respect to addition and multiplication.

Suppose \( z, w \in P \). We need to show that \( \overline{z + w} > 0 \) and \( \overline{zw} > 0 \). However, \( \overline{z + w} = \overline{z} + \overline{w} \) and \( \overline{zw} = \overline{z} \cdot \overline{w} \). So the result follows from the fact that in \( \mathbb{R} \), the product or sum of two positive numbers is again positive.

We now show that trichotomy holds. Suppose \( z \in \mathbb{Q}(\sqrt{2}) \). Note that \( \overline{-z} = -a + b\sqrt{2} = -z \) and \( -z \) is in \( P \). We need to show that if \( z \neq 0 \), then exactly one of \( z \) or \( -z \) belongs to \( P \). If \( z \in P \), then \( -z = -\overline{z} < 0 \) and so \( -z \notin P \). If \( -z \in P \), then \( 0 < -\overline{z} = -z \). Thus, we have \( \overline{z} < 0 \) (why?) and \( z \notin P \).
**Book Problem** Chapter 28: 8 (Note: by convention, if we also assume that \( F \) has an order structure, then when \( a \neq 0 \) has two square roots, we call the positive square root \( \sqrt{a} \).)

Suppose \( a \in F \). Any square root of \( a \) must satisfy the equation \( x^2 = a \). Thus, if \( a = b^2 \), then any solution must satisfy \( x^2 - b^2 = 0 \). From Equation (28) this is equivalent to requiring

\[
(x - b)(x + b) = 0.
\]

Thus, \( x \) must satisfy \( (x - b) = 0 \) or \( (x + b) = 0 \). Consequently, an element of a field has at most two square roots.

(a) If \( a = 0 \), then \( b = 0 \) is a square root of \( a \). Any other solution is of the form \( x = 0 \) or \( x = -a \). As \( -a = 0 \) (why?) we conclude that \( 0 \) has exactly one square root.

(Another line of reasoning: We show more generally that if \( c, d \) are two nonzero elements of \( F \), then \( cd \neq 0 \). Suppose that \( cd = 0 \). Since \( c \) and \( d \) are nonzero, they have multiplicative inverses \( c^{-1} \) and \( d^{-1} \), respectively. We have

\[
1 = 11 = (c^{-1}c)(dd^{-1}) = [(c^{-1}c)d^{-1}] = [c^{-1}(cd)]d^{-1} = [c^{-1}0]d^{-1} = 0d^{-1} = 0.
\]

But, \( 0 \neq 1 \).

(b) Suppose \( a \neq 0 \) has a square root \( b \). By our preliminary remarks, any other square root looks like \( b \) or \( -b \). When will \( b = -b \)? We claim this happens if and only if \( 1 + 1 = 0 \). First, since \( a \neq 0 \), we have \( b \neq 0 \). (If \( b = 0 \), then \( a = b^2 = bb = 0b = 0 \).) To prove our claim: \( b = -b \) if and only if \( b + b = 0 \) if and only if \( b1 + b1 = 0 \) if and only if \( 1 + 1 = 0 \). As \( b \) is not zero, it must be the case that \( 1 + 1 \) is zero if and only if \( b = -b \).

**Book Problem** Chapter 1: 3

(i) - (iii) see book, (iv): Since \( c \) and \( d \) are nonzero, \( cd \) is nonzero (see parenthetical remark in the proof of 28:8(a).) We have

\[
\frac{a}{b} \cdot \frac{c}{d} = (ab^{-1})(cd^{-1}) = [(ab^{-1})c]d^{-1} = [a(b^{-1}c)]d^{-1} = [a(c^{-1}b)]d^{-1} \frac{c}{d}.
\]

from (iii)

\[
= (ac)(bd)^{-1} = (ac)(db)^{-1} = \frac{ac}{db}.
\]

(v), see book (vi): We have \( \frac{a}{b} = \frac{c}{d} \) if and only if \( ab^{-1} = cd^{-1} \). Since \( d \neq 0 \), multiplying both sides by \( d \) on the right yields (see bottom of page 6): \( \frac{a}{b} = \frac{c}{d} \) if and only if

\[
(ad)b^{-1} = a(db^{-1}) = a(b^{-1}d) = (ab^{-1})d = (cd^{-1})d = c(d^{-1}d) = c1 = c.
\]

Since \( b \neq 0 \), multiplying both sides of this equation by \( b \) yields: \( \frac{a}{b} = \frac{c}{d} \) if and only if

\[
ad = (ad)1 = (ad)(b^{-1}b) = [(ad)b^{-1}]b = [c]b = cb = bc.
\]

To examine \( \frac{a}{b} = \frac{b}{a} \) we first assume that \( a \) and \( b \) are nonzero so that the expression makes sense. From the previous paragraph, we have that \( \frac{a}{b} = \frac{b}{a} \) if and only if \( a^2 = b^2 \). From our solution to Chapter 28:8, it follows that these two fractions are equal if and only if \( b = \pm a \).

**Book Problem** Chapter 1: 5(iv) – (vii)

(iv): We are given that \( b - a \in P \) and \( c \in P \). We need to show that \( bc - ac \in P \). Since \( bc - ac = cb - ca = c(b - a) \), it is enough to show that \( c(b - a) \in P \). However, this follows from the fact that \( P \) is closed with respect to multiplication.
(v) see book, (vi) Since $a > 1$ and $1 > 0$ we have $a > 0$. Thus, we have $a - 1 \in P$ and $a \in P$. We wish to conclude that $a^2 - a \in P$. Since $a^2 - a = aa - a1 = a(a - 1)$, it is enough to show that $a(a - 1) \in P$. However, this follows from the fact that $P$ is closed with respect to multiplication.

(vii) see book

**Book Problem** Chapter 1: 12 (iv) – (vi)
(iv) Let $w = -y$. The triangle inequality tells us:

$$|x + w| \leq |x| + |w|.$$ Substituting, we arrive at

$$|x - y| \leq |x| - |-y| = |x| + |y|.$$ 

(v): see book, (vi): Note that $||x| - |y||$ is either $|x| - |y|$ or $|y| - |x|$. From part (v), both of these differences are less than or equal to $|x - y| = |y - x|$. 
