Math 112 Homework 1 Solutions

Problem 1.

By contradiction: take \( r \) rational, \( x \) irrational, and assume \( y = r + x \in \mathbb{Q} \). Since \( y \in \mathbb{Q} \), \( r \in \mathbb{Q} \) and \( \mathbb{Q} \) is a field, \( x = y - r \in \mathbb{Q} \); contradiction, hence \( y \) is irrational.

Similarly, take \( r \neq 0 \) rational, \( x \) irrational, and assume \( y = rx \in \mathbb{Q} \). Since \( y \in \mathbb{Q} \), \( r \in \mathbb{Q} \), \( r \) is non-zero and \( \mathbb{Q} \) is a field, \( x = y/r \in \mathbb{Q} \); contradiction, hence \( y \) is irrational.

Problem 2.

Since \( A \) is bounded below, \( -A \) is bounded above (because if \( x \) is a lower bound of \( A \), i.e. \( x \leq y \) \( \forall y \in A \), then \( -x \geq -y \) \( \forall y \in A \), so \( -x \) is an upper bound of \( -A \)). Since \( A \) is not empty, \( -A \) is not empty either. Therefore, by the least upper bound property of \( \mathbb{R} \), the set \( -A \) admits a least upper bound \( \alpha = \text{sup}(-A) \). We must show that \( \inf(A) = -\alpha \).

First we show that \( -\alpha \) is a lower bound of \( A \). Let \( x \) be any element of \( A \): then \( -x \in -A \), so \( -x \leq \alpha \) (\( \alpha \) is an upper bound of \( -A \)). Multiplying by \(-1\) we get \( x \geq -\alpha \); since this holds for any \( x \in A \), we get that \( -\alpha \) is a lower bound of \( A \).

Next we show that \( -\alpha \) is the greatest lower bound of \( A \). Let \( y \) be any lower bound of \( A \): then \( \forall x \in A \), \( x \geq y \), so \( -x \leq -y \). Since all elements of \( -A \) are of the form \( -x \) where \( x \in A \), we get that \( -y \) is an upper bound of \( -A \). Therefore, \( -y \geq \alpha \) (because \( \alpha \) is the least upper bound). Multiplying by \(-1\) again we get \( y \leq -\alpha \), so \( -\alpha \) is the greatest lower bound of \( A \).

Problem 3.

We must check that the two axioms of an order relation (§1.5 of Rudin) hold:

(i) Let \( z = a + bi \), \( w = c + di \in \mathbb{C} \). We must show that exactly one of the three properties \( z \prec w \), \( z = w \) and \( w \prec z \) holds. There are three cases to consider: if \( a < c \), then \( z \prec w \) (while \( z \neq w \) and \( w \not< z \)); if \( a > c \), then \( w < z \) (while \( z \neq w \) and \( z \not< w \)); the last case is \( a = c \). When \( a = c \), there are again three subcases: if \( b < d \) then \( z < w \) (while \( z \neq w \) and \( w \not< z \)); if \( b > d \) then \( w < z \) (while \( z \neq w \) and \( z \not< w \)); if \( b = d \) then \( w = z \) (while \( z \not< w \) and \( w \not< z \)).

(ii) Let \( z = a + bi \), \( w = c + di \), \( u = e + fi \in \mathbb{C} \). Assume that \( z \prec w \) and \( w \prec u \). We must show that \( z \prec u \). We know that \( a \leq c \) and \( c \leq e \), therefore \( a \leq e \). If \( a < e \) then by definition \( z \prec u \).

The remaining case to consider is when \( a = e \), where \( c \) is also necessarily equal to \( a \) and \( e \); then we must have \( b < d \) and \( d < f \), so \( b < f \), and therefore \( z \prec u \).

This ordered set does not have the least-upper-bound property: for example consider \( A = \{a + bi \mid a < 0\} \): then \( c + di \) is an upper bound of \( A \) if and only if \( c \geq 0 \). However, given any upper bound \( w = c + di \) of \( A \), then \( w' = c + (d - 1)i \) is also an upper bound of \( A \) (since \( c \geq 0 \)), and \( w' < w \) (since \( d - 1 < d \)). So there is no least upper bound of \( A \).

Problem 4.

(a) Since \( \mathbb{Q}(\sqrt{2}) \) is a subset of \( \mathbb{R} \), the usual commutativity, associativity and distributivity properties are clearly satisfied. Moreover it is obvious that 0 and 1 belong to \( \mathbb{Q}(\sqrt{2}) \); therefore it is enough to check that the usual operations are well-defined in \( \mathbb{Q}(\sqrt{2}) \) (axioms (A1), (A5), (M1), (M5) of Rudin §1.12).
Let \( x = a + b\sqrt{2} \) and \( y = c + d\sqrt{2} \) be two elements of \( \mathbb{Q}(\sqrt{2}) \). Then

\[
x + y = (a + c) + (b + d)\sqrt{2}, \quad xy = (ac + 2bd) + (ad + bc)\sqrt{2}, \quad -x = (-a) + (-b)\sqrt{2}
\]

are clearly elements of \( \mathbb{Q}(\sqrt{2}) \).

Moreover, if \( x \neq 0 \), i.e. if \( a \) and \( b \) are not simultaneously equal to 0, then \( a^2 - 2b^2 \neq 0 \) because there is no rational number \( r \in \mathbb{Q} \) with the property that \( r^2 = 2 \); therefore

\[
x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2} \in \mathbb{Q}(\sqrt{2}).
\]

Therefore \( \mathbb{Q}(\sqrt{2}) \) with the usual operations is a subfield of \( \mathbb{R} \).

(b) By contradiction: assume that \( \sqrt{3} \in \mathbb{Q}(\sqrt{2}) \), i.e. there exist \( a, b \in \mathbb{Q} \) such that \( \sqrt{3} = a + b\sqrt{2} \). Then \( (a + b\sqrt{2})^2 = (a^2 + 2b^2) + 2ab\sqrt{2} \), so one gets

\[
3 - a^2 - 2b^2 = 2ab\sqrt{2}.
\]

Since \( \sqrt{2} \notin \mathbb{Q} \) the only possibility is that \( 2ab = 0 \), which implies that either \( a = 0 \) or \( b = 0 \). If \( a = 0 \) then one gets \( \sqrt{3} = b\sqrt{2} \), i.e. \( \sqrt{6} = 2b \in \mathbb{Q} \), which is a contradiction. If \( b = 0 \) then one gets \( \sqrt{3} = a \in \mathbb{Q} \), which is again a contradiction. Therefore \( \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \).

(We omit the proof that \( \sqrt{3} \) and \( \sqrt{6} \) are irrational, which is similar to that for \( \sqrt{2} \) given in Rudin).

**Problem 5.**

Recall that \( |z|^2 = z\bar{z} \). Then:

\[
|1 + z_1|^2 + |1 + z_2|^2 + \cdots + |1 + z_n|^2
= (1 + z_1)(1 + \bar{z}_1) + (1 + z_2)(1 + \bar{z}_2) + \cdots + (1 + z_n)(1 + \bar{z}_n)
= (1 + z_1 + \bar{z}_1 + |z_1|^2) + (1 + z_2 + \bar{z}_2 + |z_2|^2) + \cdots + (1 + z_n + \bar{z}_n + |z_n|^2)
= n + (|z_1|^2 + |z_2|^2 + \cdots + |z_n|^2) + (\bar{z}_1 + \bar{z}_2 + \cdots + \bar{z}_n).
\]

Since \( z_1 + z_2 + \cdots + z_n = 0 \) one also has that \( \bar{z}_1 + \bar{z}_2 + \cdots + \bar{z}_n = 0 \). In addition \( |z_1| = |z_2| = \cdots = |z_n| = 1 \), so the sum above is equal to \( 2n \).

**Problem 6.**

For \( \mathbf{x} = 0 \) the statement clearly holds (any non-zero \( \mathbf{y} \in \mathbb{R}^k \) satisfies \( \mathbf{x} \cdot \mathbf{y} = 0 \)). So we can restrict ourselves to the case where \( \mathbf{x} \neq 0 \), i.e. \( \mathbf{x} = (x_1, \ldots, x_k) \) where at least one of the \( x_i \) is non-zero. By permuting the components if necessary, we can assume without loss of generality that \( x_1 \neq 0 \).

Then let \( \mathbf{y} = (-x_2, x_1, 0, \ldots, 0) \in \mathbb{R}^k \): we have that \( \mathbf{y} \neq 0 \) (its second component is non-zero), and \( \mathbf{x} \cdot \mathbf{y} = -x_1x_2 + x_2x_1 = 0 \).

(Or more geometrically: for \( \mathbf{x} \neq 0 \), the set \( \{ \mathbf{y} \in \mathbb{R}^k, \mathbf{x} \cdot \mathbf{y} = 0 \} \) is a hyperplane, which always contains non-zero elements when \( k \geq 2 \)).

For \( k = 1 \) this is no longer true: if \( x \) is non-zero, then the equation \( x \cdot y = 0 \) admits \( y = 0 \) as only solution.
Problem 7.
For every positive integer \( n \), let \( M_n \) be the set whose elements are all the subsets of the finite set \( \{-n, \ldots, n\} \). The set \( M_n \) is finite (in fact it has \( 2^{2n+1} \) elements). However, every finite subset of \( \mathbb{Z} \) is bounded and therefore contained in \( \{-n, \ldots, n\} \) for some integer \( n \) (of course \( n \) depends on the chosen subset). So every element of \( M \) belongs to \( M_n \) for some \( n \), and therefore \( M = \bigcup_{n=1}^{\infty} M_n \).

Since it is a countable union of finite sets, \( M \) is at most countable; since \( M \) is clearly infinite, it is countable.

Alternative solution: for every integer \( n \geq 0 \), let \( A_n \) be the set of all subsets of \( \mathbb{Z} \) containing exactly \( n \) elements. The set \( A_0 \) admits the empty subset as its only element and is therefore finite. If \( n \geq 1 \), then to an element \( \{x_1, \ldots, x_n\} \) of \( A_n \) we can associate the element \( (x_1, \ldots, x_n) \) of \( \mathbb{Z}^n \) (the set of \( n \)-tuples of integers), where the \( x_i \)'s are ordered so that \( x_1 < x_2 < \cdots < x_n \). This defines a 1-1 mapping of \( A_n \) into \( \mathbb{Z}^n \). However \( \mathbb{Z}^n \) is countable (see Rudin §2.13), so \( A_n \) which is equivalent to an infinite subset of \( \mathbb{Z}^n \) is also countable. We conclude that \( M = \bigcup_{n=0}^{\infty} A_n \) is also countable.