MATH 226 - HW 1

Anish Lakkapragada – anish.lakkapragada@yale.edu – al2778

September 5, 2024

1.

(a)

Given that image b is the output of $f(a)$ where pre-image $a \in A$, $g(b)$ will always equal a as it is guaranteed that there exists a pre-image a which by function f will map to b. Thus, for all $a \in A$, $g \circ f(a) = a$ and so g is a left inverse of f.

(b)

For g to be the right inverse of f, $f \circ g(b) = b$ where we assume $b \in B$. Because f is an injective function, it is not guaranteed that every image in set B has a corresponding pre-image is in set A as defined by function f. If the given aforementioned b does not have a pre-image in set A as defined by function f, $g(b) = a_0$. And because it is not guaranteed $f(a_0)$ equals b, it is not guaranteed $f(g(b)) = b$. Thus g may not be the right inverse of f.

g would be the right inverse of f is there was a one-to-one correspondence between each pre-image in A and image B through function f. This would occur if f was a bijective function.

(c)

Given the surjective function $f : A \to B$, the right inverse is given by $g(b)$ where $f \circ g(b) = b$. The set of pre-images in A that map by function f to image $b \in B$ is given by the set $P = \{x | f(x) = b\}$. Because f is surjective, $|P| \geq 1$. In cases where $|P| > 1$, $g(b)$ must be able to choose one pre-image from P. I define $g(b)$ as taking any arbitrary pre-image from set P. Because f is surjective, $g(b)$ is guaranteed to return a pre-image that maps by function f to b. Thus the right inverse condition $f \circ g(b) = b$ is upheld, and so $g(b)$ is proved as the right inverse of f.

2.

(a)

We are given that the composition of g with f, $g \circ f$, maps set A to C. This composition $g \circ f$ is injective if any image in C has at most one pre-image in set A. If we assume f is an injective function, we know that only certain pre-images in set A will map to unique elements in set B. Similarly, if we assume g is an injective function, we know that only certain pre-images in set B will map to unique elements in set C. Because we know a subset of pre-images in A will map to a subset of unique images in B, and a subset of those images (now pre-images) in B will map to unique images in C, we know the composition function $g \circ f$ will map a subset of the pre-images in A to unique images in C. By definition, $g \circ f$ is an injective function if f and g are both injective.

(b)

If we know g is a surjective function, we know that for each image in C, there exists at least one pre-image in B. Similarily, if we know that f is a surjective function, we know that for each of these pre-images that exist in B that map to images in C, there exists at least one pre-image in A. Because every element in C is guaranteed to have at least one pre-image in A by the function $g \circ f$, by defintion, $g \circ f$ is a surjection if f and g are both surjective.

(c)

If functions f and g are both bijective, both functions map all pre-images in A and B respectively to unique images in B and C respectively. Because f provides a one-to-one correspondence between elements in A and B and g provides a one-to-one correspondence between elements in B and C, a one-to-one correspondance is maintained between each pre-image in A and image in C through the function $g(f(a))$ or $g \circ f$. Thus $g \circ f$ is a bijective function if f and g are both bijective.

3.

(a)

Let us define $x = m_1 + n_1\sqrt{2}$, where $m_1, n_1 \in \mathbb{Z}$ and $y = m_2 + n_2\sqrt{2}$, where $m_2, n_2 \in \mathbb{Z}$. Given these definitions, $x + y = (m_1 + m_2) + (n_1 + n_2)\sqrt{2}$. Because $(m_1 + m_2), (n_1 + n_2) \in \mathbb{Z} \Rightarrow x + y \in B$ if $x, y \in B$.

(b)

Let us define x and y the same as in the above part (a). Given these definitions, $xy = m_1m_2 + m_1n_2\sqrt{2} + m_2n_1\sqrt{2} + 2n_1n_2 = (2n_1n_2 + m_1m_2) + (m_1n_2 + m_2n_1)\sqrt{2}$. Because $(2n_1n_2 + m_1m_2), (m_1n_2 + m_2n_1) \in \mathbb{Z} \Rightarrow xy \in B$ if $x, y \in B$.

(c)

For the base case $k = 1$, $(-1 + \sqrt{2})^k = (-1 + \sqrt{2}) \in B$. Given integer $k \geq 1$ and $(-1 + \sqrt{2})^k \in B$, $(-1 + \sqrt{2})^{k+1} \in B$. This is because $(-1 + \sqrt{2})^{k+1} = (-1 + \sqrt{2})^k * (-1 + \sqrt{2})$ and both factors $(-1 + \sqrt{2})^k, (-1 + \sqrt{2}) \in B$. As proven in (b), B is closed under multiplication and so when both factors are in B, their product will be in B. Thus, as proven by induction, for all integers $k \geq 1$, $(-1 + \sqrt{2})^k \in B$.

4.

(a)

Note that for any set C with N items, $T(\Sigma_{i=1}^{N} C_i)$ will equal $\Sigma_{i=1}^{N} T(C_i)$ due to T being an additive function.

For all given integers $n \geq 1$:

$$T(\Sigma_{i=1}^n x) = \Sigma_{i=1}^n T(x)$$
$$T(nx) = nT(x)$$

(b)

$$T(x+y) = T(x) + T(y)$$
$$T(0+0) = T(0) + T(0)$$
$$T(0) = 2T(0)$$
$$T(0) = 0$$

(c)

$$T(x+y) = T(x) + T(y)$$
$$T(x+(-x)) = T(x) + T(-x)$$
$$T(0) = T(x) + T(-x)$$
$$0 = T(x) + T(-x)$$
$$T(x) = -T(-x)$$

(d) For all integers n and all integers $k \neq 0$,

$$T((\frac{n}{k} * k)x) = \Sigma_{i=1}^k T(\frac{n}{k}x) = kT(\frac{n}{k}x)$$

If we define r to be the fraction $\frac{n}{k}$, by definition $r \in \mathbb{Q}$ as n and k are both integers where denominator $k \neq 0$. Using r, we can simplify the above expression further:

$$T(nx) = \frac{n}{r}T(rx)$$
$$rT(nx) = nT(rx)$$

As n is defined as $n \in \mathbb{Z}$, we first generalize our proof in (a) that $T(nx) = nT(x)$ from all integers $n \geq 1$ to $n \in \mathbb{Z}$. Given an integer $n < 0$, if $u = nx$, we can use our proof in (c) that for $u \in \mathbb{R}$, $T(u) = -T(-u)$ and thus since $T(-u) = T(|n|x) = |n|T(x)$, we can conclude that in cases where $n < 0$, $T(u) = T(nx) = -|n|T(x) = nT(x)$ or more simply, $T(nx) = nT(x)$. And in cases where $n = 0$, $T(nx) = nT(x)$ as $T(0) = 0$ as proven in (b). Thus our proof in (a) is generalized to $n \in \mathbb{Z}$. Using this result, we can continue simplifying our above expressions.

$$r(nT(x)) = nT(rx)$$
$$rT(x) = T(rx)$$
$$T(rx) = rT(x)$$

for all rational numbers $r \in \mathbb{Q}$.

(e)

Let us define $T(x)$:

$$T(x) = \begin{cases} x, & \text{if } x \in \mathbb{Q} \\ 0, & \text{if } x \notin \mathbb{Q} \end{cases}$$

Defining $r = \sqrt{2}, x = 1$:

$$\begin{gathered} T(\sqrt{2}x) = \sqrt{2}T(x) \\ T(\sqrt{2}) = \sqrt{2} * T(1) \\ 0 \neq 1 \\ T(rx) \neq rT(x) \end{gathered}$$

As proven by contradiction, $T(rx) \neq rT(x)$ for all reals $r \in \mathbb{R}$.

5.

(a)

Let us define field $\mathbb{F} = (\mathbb{Z}\{\sqrt{3}\}, +, \cdot)$ and the multiplicative inverse of $a + b\sqrt{3}$ as z where $(a + b\sqrt{3})z = 1$. Given that $a^2 - 3b^2 \neq 0$, z is given by $\frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2}$. In the case where $a^2 - 3b^2 = 1$, $z = a - b\sqrt{3}$. Because $a - b\sqrt{3} \in \mathbb{F}$, $a + b\sqrt{3}$ has a multiplicative inverse in this case. Similarily, in the case where $a^2 - 3b^2 = -1$, $z = -a + b\sqrt{3}$. Because $-a + b\sqrt{3} \in \mathbb{F}$, $a + b\sqrt{3}$ has a multiplicative inverse in this case as well.

(b)

Given that $a + b\sqrt{3} \in \mathbb{F}$ has a multiplicative inverse, let us define this multiplicative inverse as $c + d\sqrt{3} \in \mathbb{F}$ where $c, d \in \mathbb{Z}$ and $(a + b\sqrt{3})(c + d\sqrt{3}) = 1$. Let us also define the greatest common divisor of a and b as $k = gcd(a, b) \in \mathbb{Z}$ where $a = ka'$ and $b = kb'$ and $a', b' \in \mathbb{Z}$ are coprime. We inspect the possible values of k below.

$$\begin{gathered} (a + b\sqrt{3}) * (c + d\sqrt{3}) = 1 \\ (ka' + kb'\sqrt{3}) * (c + d\sqrt{3}) = 1 \\ ka'c + ka'd\sqrt{3} + kb'c\sqrt{3} + 3kb'd = 1 + 0\sqrt{3} \\ ka'c + 3kb'd = 1 \\ k(a'c + 3b'd) = 1 \\ (a'c + 3b'd) = \frac{1}{k} \end{gathered}$$

Because $a'c + 3b'd \in \mathbb{Z} \Rightarrow k \leq 1$. Because $k \in \mathbb{Z} \Rightarrow k = 1$. We now define the values of c, d in terms of a, b. Defining $z = c + d\sqrt{3}$, $z = \frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} \Rightarrow c = \frac{a}{a^2-3b^2}, d = \frac{-b}{a^2-3b^2}$. Because the largest possible value that can divide two integers, a, b, into integers is given by $k = gcd(a, b)$, the denominator in c, d of $a^2 - 3b^2$ must equal $k = 1$ in order to ensure $c, d \in \mathbb{Z}$ so that $c + d\sqrt{3} \in \mathbb{F}$. Note that $a^2 - 3b^2 = -1$ also ensures the multiplicative inverse $c + d\sqrt{3} \in \mathbb{F}$ as $c, d \in \mathbb{Z}$ because $\pm a, \pm b \in \mathbb{Z}$. Thus, if $a + b\sqrt{3} \in \mathbb{F}$ has a multiplicative inverse, we know that $|a^2 - 3b^2| = 1$. If there is no multiplicative inverse in $\mathbb{F}$, that is because $c \notin \mathbb{Z}$ or $d \notin \mathbb{Z}$, which would happen only if the denominator $|a^2 - 3b^2| \neq gcd(a, b)$ or $|a^2 - 3b^2| \neq 1$. Thus, if $a + b\sqrt{3} \in \mathbb{F}$ has a multiplicative inverse $\Longleftrightarrow |a^2 - 3b^2| = 1$.

(c)

In order for $\mathbb{F} = (\mathbb{Z}\{\sqrt{3}\}, +, \cdot)$ to define a field, $\forall m \in \mathbb{F}$, $\exists n \in \mathbb{F}$ such that $m \cdot n = 1$. However, as shown in (b), $a + b\sqrt{3} \in \mathbb{F}$ will only have a guaranteed multiplicative inverse in the special case that $|a^2 - 3b^2| = 1$. Thus, $\mathbb{F}$ fails to meet the muliplicative inverse condition to be defined as a valid field.