Dmitry Vaintrob

Math 113 PSet 1
Solutions

① Proof of ($\Rightarrow$).

We are given that f is a bijection.
It is a surjection, so $\forall y \in T \ \exists x \in S$ such that $f(x) = y$.

For each $y \in T$, pick one such x (in fact, by the injective property, it is unique), and call it $g(y)$. The assignment $y \mapsto g(y)$ defines a function

$$g : T \to S.$$

Now we must check that g is both a left inverse and a right inverse to f.

(i) (right inverse) Need to compare $f \circ g : T \to T$ and $id_T : T \to T$, i.e. compare every value.
Take any $y \in T$.
By our construction of g, the element $x = g(y)$ satisfies $f(x) = y$. So
$$f \circ g(y) = f(g(y)) = f(x) = y = id_T(y)$$
and we have checked (by comparing every value) that $f \circ g = id_T$.

(ii) (left inverse) Need to compare $g \circ f : S \to S$ and $id_S : S \to S$.
Let $x \in S$ be any element.
Set $x' = g(f(x))$.
By construction of g, the element $x' \in S$ satisfies $f(x') = f(x)$.
By injectivity, $x' = x$.
So $\forall x \in S$ we have shown $g \circ f(x) = x = id_S\, x$.
Therefore $g \circ f = id_S : S \to S$

This completes the proof of the ($\Rightarrow$) direction (the statement that $f: S \to T$ with f a bijection $\Rightarrow \exists\, g: T \to S$ satisfying $f \circ g = id_T$ and $g \circ f = id_S$.

Next, we prove the ($\Leftarrow$) direction.

We are given

$f: S \to T$ and the statement that

$\exists\, g: T \to S$ such that $f \circ g = id_T$ and $g \circ f = id_S$.

Pick such a g once and for all

<note: it turns out that when it exists, the function g is unique, but we will not prove that here.>

We want to deduce that f is bijective.

There are two things to prove: surjectivity and injectivity.

(Surjectivity): $\forall\, y \in T$, let $x = g(y)$.

Then $f(x) = f(g(y)) = id_T(y) = y$,

so every $y \in T$ is hit and f is surjective.

(Injectivity): Assume that $f(x) = f(x')$ for $x, x' \in S$. Applying g to the equality:

$g(f(x)) = g(f(x'))$ so

$g \circ f(x) = g \circ f(x')$ and using $g \circ f = id_S$

we deduce

$x = g \circ f(x) = g \circ f(x') = x'$, so $x = x'$.

This concludes the proof of injectivity of f.

Surjectivity and injectivity imply bijectivity.

This concludes the proof of the ($\Rightarrow$) direction of the if and only if statement. Having proven both directions, we are done.

② (a)

(*) $(a:b) + (c:d) = (ad + bc : bd)$ by the rule.

(**) $(a':b') + (c:d) = (a'd + b'c : b'd)$.

Equivalence $(a:b) \sim (a':b')$ means

(***) $ab' = a'b$.

To check equivalence of sums need to show that (*) $\sim$ (**), in other words show equality of

$(ad + bc)\cdot(b'd)$ and $(a'd + b'c)\cdot bd$.

Expand $(ad + bc)(b'd)$

$= adb'd + bcb'd = \boxed{ab'}d^2 + bb'cd$ (****)

Using (***), $= \boxed{a'b}d^2 + bb'cd$.

Now expand $(a'd + b'c)\cdot bd$

$= a'bd^2 + bb'cd =$ (****)

$= (ad + bc)b'd$, as desired. Therefore,

$(a:b) + (c:d) \sim (a':b') + (c:d)$.

(b) Using the obvious commutativity of the expression for $(x:y) + (z:t)$, we can deduce that if

$(c:d) \sim (c':d')$ then

$(a:b) + (c:d) \sim (a:b) + (c':d')$.

Applying both of these together:

$(a:b) + (c:d) \sim (a':b') + (c:d) \sim (a':b') + (c':d')$,

So replacing both sides of the sum by 'equivalent' fractions produces an 'equivalent' result, as desired.

2(c) (EC)

We would like to show that $(a:b) \sim (a':b')$ iff $\frac{a}{b} = \frac{a'}{b'}$ in reduced terms, i.e. iff $\frac{a}{b} = \frac{a_0 \cdot d}{b_0 \cdot d}$ and $\frac{a'}{b'} = \frac{a_0 \cdot d'}{b_0 \cdot d'}$ for some relatively prime a_0, b_0 with $b_0 > 0$.

Start with the ($\Leftarrow$) direction:
$(a_0 \cdot d : b_0 \cdot d) \sim (a_0 \cdot d' : b_0 \cdot d')$ by checking $a_0 d b_0 d' = b_0 d a_0 d'$.

Now to check the ($\Rightarrow$) direction:
We are given $(a:b) \sim (a':b')$.
Let $\frac{a_0}{b_0}$ be $\frac{a}{b}$ in reduced terms.
Then a_0 and b_0 are relatively prime, $b_0 > 0$, and $\exists\, d \in \mathbb{Z}^*$ such that $a = a_0 \cdot d$ and $b = b_0 \cdot d$
<this is the definition of a fraction in reduced terms>. Now
$d a_0 b' = a b' = a' b = d a' b_0$, so $a_0 b' = a' b_0$. $(*)$
Since a_0, b_0 are relatively prime, $(*)$ implies $a_0 \mid a'$ and $b_0 \mid b'$.
Say $a' = a_0 \cdot x$ and $b' = b_0 \cdot y$. Then
$(*) \Rightarrow a_0 b_0 y = a_0 b_0 \cdot x$, so $x = y$. So:
For some integer x, $a' = x \cdot a_0$ and $b' = x \cdot b_0$.
This means $\frac{a'}{b'} = \frac{a_0}{b_0}$ in reduced terms

[Shorter proof using knowledge of real numbers in reduced terms <also allowed>: $a/b = a'/b'$ as real numbers. Multiplying
$\Leftrightarrow$ $a/b = a'/b'$ both sides by the nonzero number bb', this is equivalent to $ab' = a'b$]

(3) (a) $a' \equiv_4 a \iff \exists k \in \mathbb{Z} \mid a'-a = 4k$

$b' \equiv_4 b \iff \exists l \in \mathbb{Z} \mid b'-b = 4l.$

then $a'+b' = a+b + 4(k+l)$ so

$a'+b' \equiv_4 a+b.$

(b) ($\Leftarrow$) assume a and a' have the same remainder modulo 4. Then there is some $r \in \{0,1,2,3\}$ such that $a = 4 \cdot k + r$ and $a' = 4 \cdot k' + r$.

Now $a' - a = 4k' + r - (4k + r) = 4(k'-k)$, so (since $k', k \in \mathbb{Z}$) we see $a' \equiv_4 a$.

($\Rightarrow$) Assume $a \equiv_4 a'$. Let r, r' be the remainders of a, respectively, a', when divided by 4. Then (for some $k, k' \in \mathbb{Z}$) we have $a = 4k + r$, $a' = 4k' + r'$, and the equivalence $a \equiv_4 a'$ implies $\exists\, l \in \mathbb{Z}$ with $a' - a = 4 \cdot l$. So:

$4l = a' - a = (4k' + r') - (4k + r) = 4(k'-k) + r' - r$

So: $r' - r = 4l - 4(k'-k) = 4(l + k - k')$.
(which is divisible by 4).
The difference between two numbers between 0 and 3 is (in absolute value) at most 3, so the only way it can be a multiple of 4 is if this difference is 0 and $r = r'$.