MTH 505 Homework 1

Roy Howie

February 1, 2017

1 Developing $\mathbb{N}$

Completed in the following order: a, b, c, d, e, h, f, g.

(a) Let $S = \{n \in \mathbb{N} \mid n = 0 \ \vee \ \exists m \in \mathbb{N} \text{ such that } \sigma(m) = n\}$. Note $0 \in S$. Next, suppose $x \in S$, then $\sigma(x) \in S$, as there exists $m \in \mathbb{N}$ such that $\sigma(m) = \sigma(x)$: namely, x itself. Hence, **P4** $\Rightarrow S = \mathbb{N}$.

Next, fix $n \in \mathbb{N}$ and suppose $\exists m_1, m_2 \in \mathbb{N}$ such that $\sigma(m_1) = n = \sigma(m_2)$ and $m \neq n$. This is a contradiction. By **P3**, $\sigma(m_1) = \sigma(m_2)$ implies $m_1 = m_2$. Hence, predecessors are unique. $\square$

(b) Fix $a, b \in \mathbb{N}$ and let $S = \{c \in \mathbb{N} \mid a+(b+c) = (a+b)+c\}$. By (**1**), $0 \in S$ as $a+(b+0) = a+(b) = (a+b)+0$. Next, suppose $n \in S$, then

$$\begin{aligned} a + (b + \sigma(n)) &= a + \sigma(b+n) && (2) \\ &= \sigma(a + (b+n)) && (2) \\ &= \sigma((a+b)+n) && (\text{IH}) \\ &= (a+b) + \sigma(n) && (2) \end{aligned}$$

Hence, $\sigma(n) \in S$, so **P4** $\Rightarrow S = \mathbb{N}$. $\square$

(c) Let $S = \{n \in \mathbb{N} \mid 0 + n = n\}$. By (**1**), $0 \in S$ as $0 + 0 = 0$. Next, suppose $x \in S$, then

$$\begin{aligned} 0 + \sigma(x) &= \sigma(0 + x) && (2) \\ &= \sigma(x) && (\text{IH}) \end{aligned}$$

Hence, $\sigma(x) \in S$, so **P4** $\Rightarrow S = \mathbb{N}$. In addition, via (**1**), one has $0 + n = n + 0$ for all $n \in \mathbb{N}$.

Let $R = \{n \in \mathbb{N} \mid n + \sigma(0) = \sigma(0) + n\}$. By above, $0 \in R$, as $0 + \sigma(0) = \sigma(0) + 0$. Suppose $x \in R$, then

$$\begin{aligned} \sigma(x) + \sigma(0) &= \sigma(\sigma(x) + 0) && (2) \\ &= \sigma(\sigma(x)) && (1) \\ &= \sigma(\sigma(x+0)) && (1) \\ &= \sigma(x + \sigma(0)) && (2) \\ &= \sigma(\sigma(0) + x) && (\text{IH}) \\ &= \sigma(0) + \sigma(x) && (2) \end{aligned}$$

Hence, $\sigma(x) \in R$, so **P4** $\Rightarrow R = \mathbb{N}$. $\square$

(d) Fix $a \in \mathbb{N}$ and let $S = \{b \in \mathbb{N} \mid a + b = b + a\}$. By **(c)**, $0 \in S$. Suppose $x \in S$, then

$$\begin{aligned}
a + \sigma(x) &= \sigma(a + x) && (2)\\
&= \sigma(x + a) && (\text{IH})\\
&= \sigma((x + a) + 0) && (1)\\
&= (x + a) + \sigma(0) && (2)\\
&= x + (a + \sigma(0)) && (\text{b})\\
&= x + (\sigma(0) + a) && (\text{c})\\
&= (x + \sigma(0)) + a && (\text{b})\\
&= \sigma(x + 0) + a && (2)\\
&= \sigma(x) + a && (1)
\end{aligned}$$

Hence, $\sigma(x) \in S$, so **P4** $\Rightarrow S = \mathbb{N}$. $\square$

(e) Fix $b, c \in \mathbb{N}$ and let $S = \{a \in \mathbb{N} \mid (b + c)a = ba + ca\}$. By **(1)** and **(3)**, $0 \in S$, as $(b + c) * 0 = 0 + 0$. Suppose $x \in S$, then

$$\begin{aligned}
(b + c)\sigma(x) &= (b + c)x + (b + c) && (4)\\
&= (bx + cx) + (b + c) && (\text{IH})\\
&= (bx + b) + (cx + c) && (\text{b,d})\\
&= b\sigma(x) + c\sigma(x) && (4)
\end{aligned}$$

Hence, $\sigma(x) \in S$, so **P4** $\Rightarrow S = \mathbb{N}$. $\square$

(f) Fix $a, b \in \mathbb{N}$ and let $S = \{c \in \mathbb{N} \mid (ab)c = a(bc)\}$. By **(3)**, $0 \in S$, as $a(b * 0) = 0 = (ab) * 0$. Suppose $x \in S$, then

$$\begin{aligned}
a(b\sigma(x)) &= a(bx + b) && (4)\\
&= a(bx) + ab && (\text{h,e})\\
&= (ab)x + ab && (\text{IH})\\
&= (ab)x + ab\sigma(0) && (\text{h})\\
&= (ab)(x + \sigma(0)) && (\text{e})\\
&= (ab)\sigma(x + 0) && (2)\\
&= (ab)\sigma(x) && (1)
\end{aligned}$$

Hence, $\sigma(x) \in S$, so **P4** $\Rightarrow S = \mathbb{N}$. $\square$

(g) By **(h)** and **(4)**, $\sigma(a)b = b\sigma(a) = ba + b = ab + b$. $\square$

(h) Let $S = \{n \in \mathbb{N} \mid 0 * a = 0\}$. By **(3)**, $0 \in S$, as $0 * 0 = 0$. Suppose $x \in S$, then

$$\begin{aligned}
0 * \sigma(x) &= 0 * n + 0 && (4)\\
&= 0 + 0 && (\text{IH})\\
&= 0 && (1)
\end{aligned}$$

Hence, $\sigma(x) \in S$, so **P4** $\Rightarrow S = \mathbb{N}$.

Let $R = \{a \in \mathbb{N} \mid \sigma(0) * a = a\}$. By **(1)**, $0 \in S$, as $\sigma(0) * 0 = 0$. Suppose $x \in S$, then

$$\begin{aligned}
\sigma(0)\sigma(x) &= \sigma(0)x + \sigma(0) && (4)\\
&= x + \sigma(0) && (\text{IH})\\
&= \sigma(x + 0) && (2)\\
&= \sigma(x) && (1)
\end{aligned}$$

Hence, $\sigma(x) \in R$, so **P4** $\Rightarrow R = \mathbb{N}$.

Fix $a \in \mathbb{N}$ and let $Q = \{b \in \mathbb{N} \mid ab = ba\}$. By above, $0 \in Q$ because $0 * a = a * 0$. Suppose $x \in Q$, then

$$\begin{aligned} a\sigma(x) &= ax + a && (4) \\ &= xa + a && \text{(IH)} \\ &= xa + \sigma(0)a && \text{(above)} \\ &= (x + \sigma(0))a && \text{(e)} \\ &= \sigma(x + 0)a && (2) \\ &= \sigma(x)a && (1) \end{aligned}$$

Hence, $\sigma(x) \in Q$, so **P4** $\Rightarrow Q = \mathbb{N}$. $\square$

Lemma. *(Additive Cancellation) For $a, b, c \in \mathbb{N}$, if $a + c = b + c$, then $a = b$.*

Proof. Fix $a, b \in \mathbb{N}$ and let $S = \{c \in \mathbb{N} \mid a + c = b + c \Rightarrow a = b\}$. Note $0 \in S$. Suppose $x \in S$, then

$$\begin{aligned} a + \sigma(x) &= b + \sigma(x) \\ \sigma(a + x) &= \sigma(b + x) && (2) \\ a + x &= b + x && \text{(P3)} \\ a &= x && \text{(IH)} \end{aligned}$$

Hence $\sigma(x) \in S$, so **P4** $\Rightarrow S = \mathbb{N}$. $\square$

2 From $\mathbb{N}$ to $\mathbb{Z}$

(a) To show $[a, b] \sim [c, d] \iff a + d = c + b$ is an equivalence relation:

(1) $[a, b] \sim [a, b] \Rightarrow a + b = a + b$

(2) $[a, b] \sim [c, d] \Leftrightarrow [c, d] \sim [a, b]$. Note that $[a, b] \sim [c, d] \Leftrightarrow a+d = c+b \Leftrightarrow c+b = a+d \Leftrightarrow [c, d] \sim [a, b]$.

(3) $[a, b] \sim [c, d] \wedge [c, d] \sim [e, f] \Rightarrow [a, b] \sim [e, f]$. By assumption, $a + d = b + c$ and $c + f = e + d$.

$$\begin{aligned} a + d &= c + b \\ (a + d) + f &= (c + b) + f \\ &= b + (c + f) \\ &= b + (e + d) \\ &= (e + b) + d \\ (a + f) + d &= (e + b) + d \end{aligned}$$

Hence, by the Additive Cancellation Lemma, $a + f = e + b$, so $[a, b] \sim [e, f]$. $\square$

(b) (1) To show $[a, b] + [c, d] = [a + c, b + d]$ is well-defined, consider $[a, b] \sim [a', b']$ and $[c, d] \sim [c', d']$. Note that $a + b' = a' + b$ and $c + d' = c' + d$. Therefore, $(a + b') + (c + d') = (a' + b) + (c' + d)$. Some shuffling of terms yields $(a + c) + (b' + d') = (a' + c') + (b + d)$, implying $[a + c, b + d] \sim [a' + c', b' + d']$, so addition on equivalence classes is indeed well-defined.

(2) To show $[a, b] * [c, d] = [ac + bd, ad + bc]$ is well-defined, again consider $[a, b] \sim [a', b']$ and $[c, d] \sim [c', d']$.

We want $[ac+bd, ad+bc] \sim [a'c'+b'd', a'd'+b'c']$, or $(ac+bd)+(a'd'+b'c') = (a'c'+b'd')+(ad+bc)$. We have $a+b' = a'+b$ and $c+d' = c'+d$. We only need imagination:

$$\begin{aligned}
(a+b')+(a'+b)+(c+d')+(c'+d) &= (a'+b)+(a+b')+(c'+d)+(c+d') \\
(a+b')c+(a'+b)d+(c+d')a'+(c'+d)b' &= (a'+b)c+(a+b')d+(c'+d)a'+(c+d')b' \\
(ac+b'c)+(a'd+bd)+(ca'+d'a')+(c'b'+db') &= (a'c+bc)+(ad+b'd)+(c'a'+da')+(cb'+d'b') \\
(ac+bd)+(d'a'+c'b')+(b'c+a'd+ca'+db') &= (c'a'+d'b')+(ad+bc)+(a'c+b'd+da'+cb') \\
(ac+bd)+(d'a'+c'b') &= (c'a'+d'b')+(ad+bc)
\end{aligned}$$

The general rule is to keep numbers of the form ab or $a'b'$ but not $a'b$ or ab'. Nevertheless, the last line implies the desired result, so multiplication on equivalence classes is well-defined. □

(c) (1) Associativity of $+ : \mathbb{Z} \to \mathbb{Z}$

$$\begin{aligned}
([a,b]+[c,d])+[e,f] &= [a+c, b+d]+[e,f] \\
&= [(a+c)+e, (b+d)+f] \\
&= [a+(c+e), b+(d+f)] \\
&= [a,b]+[c+e, d+f] \\
&= [a,b]+([c,d]+[e,f])
\end{aligned}$$

(2) Commutativity of $+ : \mathbb{Z} \to \mathbb{Z}$

$$\begin{aligned}
[a,b]+[c,d] &= [a+c, b+d] \\
&= [c+a, d+b] \\
&= [c,d]+[a,b]
\end{aligned}$$

(3) Associativity of $* : \mathbb{Z} \to \mathbb{Z}$

$$\begin{aligned}
([a,b]*[c,d])*[e,f] &= [ac+bd, ad+bc]*[e,f] \\
&= [(ac+bd)e+(ad+bc)f, (ac+bd)f+(ad+bc)e] \\
&= [ace+bde+adf+bcf, acf+bdf+ade+bce] \\
&= [a(ce+df)+b(cf+de), a(cf+de)+b(df+ce)] \\
&= [a,b]*[ce+df, cf+de] \\
&= [a,b]*([c,d]*[e,f])
\end{aligned}$$

(4) Commutativity of $* : \mathbb{Z} \to \mathbb{Z}$

$$\begin{aligned}
[a,b]*[c,d] &= [ac+bd, ad+bc] \\
&= [ca+db, cb+da] \\
&= [c,d]*[a,b]
\end{aligned}$$

□

(d) First, additive inverses are added, which turns $\mathbb{N}$ into an abelian group $\mathbb{Z}'$. Next, a second binary operation, multiplication, is added to transform the abelian group $\mathbb{Z}'$ into the commutative ring $\mathbb{Z}$. Every $n \in \mathbb{N}$ has an "additive inverse" in the form of the members of the equivalence class of $[0, n]$.

3 From $\mathbb{Z}$ to $\mathbb{Q}$

(a) To show $[a,b] \sim [c,d] \Leftrightarrow ad = bc$ is an equivalence relation:

(1) $[a,b] \sim [a,b] \Rightarrow ab = ba$

(2) $[a,b] \sim [c,d] \Leftrightarrow [c,d] \sim [a,b]$ Note that $[a,b] \sim [c,d] \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow [c,d] \sim [a,b]$.

(3) $[a,b] \sim [c,d] \wedge [c,d] \sim [e,f] \Rightarrow [a,b] \sim [e,f]$. By assumption, $ad = bc$ and $cf = de$.

$$\begin{aligned} (ad)f &= (bc)f \\ &= b(cf) \\ &= b(de) \\ (af)d &= (be)d \end{aligned}$$

Hence, by multiplicative cancellation, $af = be$, so $[a,b] \sim [e,f]$. $\square$

(b) (1) To show $[a,b] * [c,d] = [ac, bd]$ is well-defined, consider $[a,b] \sim [a',b']$ and $[c,d] \sim [c',d']$. Note that $ab' = ba'$ and $cd' = dc'$. Therefore, $(ab')(cd') = (ba')(dc')$. Shuffling terms gives $(ac)(b'd') = (bd)(a'c')$, implying $[ac, bd] \sim [a'c', b'd']$. Hence, multiplication is well-defined.

(2) To show $[a,b] + [c,d] = [ad+bc, bd]$ is well-defined, again consider $[a,b] \sim [a',b']$ and $[c,d] \sim [c',d']$.

$$\begin{aligned} (ab') + (cd') &= (ba') + (dc') \\ (bb' + dd')(ab' + cd') &= (ba' + dc')(dd' + bb') \\ (ab'dd' + cd'bb') + (ab'bb' + cd'dd') &= (a'bdd' + c'dbb') + (ba'bb' + dc'dd') \\ ab'dd' + cd'bb' &= a'bdd' + c'dbb' \\ (ad)(b'd') + (bc)(b'd') &= (a'd')(bd) + (b'c')(bd) \\ (ad + bc)(b'd') &= (bd)(a'd' + b'c') \end{aligned}$$

Hence, $[ad + bc, bd] \sim [a'd' + b'c', b'd']$ and addition is well-defined. $\square$

(c) Too tedious.

(d) $\mathbb{Z}$ is a commutative ring, whereas $\mathbb{Q}$ is a field. Thus, to transition from $\mathbb{Z}$ to $\mathbb{Q}$, one needs multiplicative inverses for all nonzero integers. Thus, every $q \in \mathbb{Q}$ is represented by an equivalence class $[a,b]$ and has a corresponding "multiplicative inverse" represented by the equivalence class $[b,a]$.