Cavallaro, Jeffery
Math 221a
Homework #1

1.1.6

Construct the addition table for $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

$\mathbb{Z}_2 = \{0, 1\}$

$$
\begin{array}{c|cccc}
\bigoplus & (0,0) & (0,1) & (1,0) & (1,1) \\
\hline
(0,0) & (0,0) & (0,1) & (1,0) & (1,1) \\
(0,1) & (0,1) & (0,0) & (1,1) & (1,0) \\
(1,0) & (1,0) & (1,1) & (0,0) & (0,1) \\
(1,1) & (1,1) & (1,0) & (0,1) & (0,0)
\end{array}
\implies
\begin{array}{c|cccc}
* & \text{e} & \text{a} & \text{b} & \text{c} \\
\hline
\text{e} & \text{e} & \text{a} & \text{b} & \text{c} \\
\text{a} & \text{a} & \text{e} & \text{c} & \text{b} \\
\text{b} & \text{b} & \text{c} & \text{e} & \text{a} \\
\text{c} & \text{c} & \text{b} & \text{a} & \text{e}
\end{array}
\implies K_4
$$

1.1.8

Let $\sim$ be a relation on $\langle \mathbb{Q}, + \rangle$ defined by: $a \sim b \iff a - b \in \mathbb{Z}$

a) Prove: $\sim$ is a congruence relation.

First, prove that $\sim$ is an equivalence relation.

R: Assume $a \in \mathbb{Q}$

$a - a = 0 \in \mathbb{Z}$
$\therefore a \sim a$

S: Assume $a \sim b$

$a - b \in \mathbb{Z}$
$-(a - b) \in \mathbb{Z}$
$b - a \in \mathbb{Z}$
$\therefore b \sim a$

T: Assume $a \sim b$ and $b \sim c$

$a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$
$(a - b) + (b - c) \in \mathbb{Z}$
$a - c \in \mathbb{Z}$
$\therefore a \sim c$

$\therefore \sim$ is an equivalence relation.

Now show that $\sim$ is a congruence relation.

Assume $a_1, a_2, b_1, b_2 \in \mathbb{Q}$
Assume $a_1 \sim a_2$ and $b_1 \sim b_2$
$a_1 - a_2 \in \mathbb{Z}$ and $b_1 - b_2 \in \mathbb{Z}$
$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in \mathbb{Z}$
$a_1 + b_1 \sim a_2 + b_2$
$\therefore \sim$ is a congruence relation.

b) Prove: $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group.

$\langle \mathbb{Q}, + \rangle$ is an abelian group (and thus a monoid)
From part (a), $\sim$ is a congruence relation on $\langle \mathbb{Q}, + \rangle$
$\therefore$ by Theorem 1.5, G/Z is an abelian group under the binary operation $\overline{a} + \overline{b} = \overline{a+b}$.

To show that G/Z is infinite, start by noting that if $a \sim b$ and $a \neq b$ then $|a - b| \in \mathbb{Z}^+$. Thus, given $a \in \mathbb{Q}$, the closest related values are $a + 1$ and $a - 1$.

Assume $a_0 \in \mathbb{Q}$ and consider the interval $(a_0, a_0 + 1)$.
a_0 is related to nothing else in this interval.

Claim: $\forall\, n \in \mathbb{N}$ there exists a unique equivalence class representative in $(a_0, a_0 + 1)$.

Proof by induction on n (the number of steps)

Base: $n = 1$

By the density of $\mathbb{Q}$ there exists a_1 not yet selected in $(a_0, a_0 + 1)$.
$|a_0 - a_1| < 1$, so $a_0 \nsim a_1$ and thus $\overline{a_0} \neq \overline{a_1}$.

Assume that n unique representatives have been selected in $(a_0, a_0 + 1)$ by selecting $a_k \in (a_0, a_{k-1})$.

Consider the $(n + 1)$ step.
By the density of $\mathbb{Q}$ there exists $a_{n+1} \in (a_0, a_n)$ not yet selected.
$|a_{n+1} - a_k| < 1, 1 \leq k \leq n$
So $a_{n+1} \nsim a_k$ and thus $\overline{a_{n+1}} \neq \overline{a_k}$.

Let A be the set of unique equivalence class representatives selected in this fashion. Since A has a one-to-one correspondence with $\mathbb{N}$, A is an infinite set. But since $A \subseteq \mathbb{Q}/\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$ is also infinite.

1.1.9

Let p be a prime number.

a) Let $R_p = \left\{ \frac{a}{b} \in \mathbb{Q} \mid (p, b) = 1 \right\}$. Prove $\langle R_p, + \rangle$ is an abelian group.

$R_p \subset \mathbb{Q}$

Assume $r = \frac{a}{b} \in R_p$
$\frac{a}{b}$ may not be in lowest form, so there is a possible issue with R_p being well-formed.

Let $\frac{a}{b} = \frac{a'}{b'}$, where $\frac{a'}{b'}$ is in lowest form.
Let $d = (a, b)$
$b' = \frac{b}{d}$
$b = b'd$
$b' \mid b$, so $(b, b') = b'$
$(p, b) = 1$
$(p, b, b') = ((p, b), b') = (1, b') = 1$
$(p, b, b') = (p, (b, b')) = (p, b')$
$(p, b') = 1$
$\therefore \frac{a'}{b'} \in R_p$ and R_p is well-defined.

Assume $r, s \in R_p$
$\exists\, a_1, b_1 \in \mathbb{Z}, r = \frac{a_1}{b_1}, b_1 \neq 0, (p, b_1) = 1$
$\exists\, a_2, b_2 \in \mathbb{Z}, s = \frac{a_2}{b_2}, b_2 \neq 0, (p, b_2) = 1$
$r + s = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \in \mathbb{Q}$
$a_1 b_2 + a_2 b_1 \in \mathbb{Z}$
$b_1 \neq 0$ and $b_2 \neq 0$ so $b_1 b_2 \neq 0$
$p \nmid b_1$ and $p \nmid b_2$ so $p \nmid b_1 b_2$
But p is prime and thus has no divisors other than p and 1, so $(p, b_1 b_2) = 1$
$\therefore r + s \in R_p$ and $\langle R_p, + \rangle$ is closed.

$\langle \mathbb{Q}, + \rangle$ is associative, so $\langle R_p, + \rangle$ is associative.

$(p, 1) = 1$, so $\frac{0}{1} \in R_p$
Assume $r = \frac{a}{b} \in R_p$
$\frac{0}{1} + r = \frac{0}{1} + \frac{a}{b} = \frac{0b + 1a}{1b} = \frac{a}{b} = r$
$r + \frac{0}{1} = \frac{a}{b} + \frac{0}{1} = \frac{1a + 0b}{1b} = \frac{a}{b} = r$
$\therefore \frac{0}{1}$ is a two-sided identity for R_p.

Assume $r = \frac{a}{b} \in R_p$
$-r = -\frac{a}{b} = \frac{(-a)}{b} \in R_p$
$-r + r = -\frac{a}{b} + \frac{a}{b} = 0 = \frac{0}{1}$
$r + (-r) = \frac{a}{b} - \frac{a}{b} = 0 = \frac{0}{1}$
$\therefore -r$ is a two-sided inverse for r.

$\langle \mathbb{Q}, + \rangle$ is commutative, so $\langle R_p, + \rangle$ is commutative.

$\therefore \langle R_p, + \rangle$ is an abelian group.

b) Let $R^p = \left\{ \frac{a}{b} \in \mathbb{Q} \mid b = p^n, n \geq 0 \right\}$ Prove $\langle R^p, + \rangle$ is an abelian group.

$R^p \subset \mathbb{Q}$

Once again, there are well-formed worries.
Assume $r = \frac{a}{b} \in R^p$.
If $\frac{a}{b}$ is not in lowest form then $\exists\, \frac{a'}{b'} \in R^p$ in lowest form such that $\frac{a}{b} = \frac{a'}{b'}$.
Assume $d = (a, b)$
$a' = \frac{a}{d}$ and $b' = \frac{b}{d}$
But all the factors of b are non-negative powers of p,

so d must also be a non-negative power of p.
Since $d \leq b$, b' must also be a non-negative power of p.
$\therefore R^p$ is well-defined.

Assume $r, s \in R_p$
$\exists\, a_1, b_1 \in \mathbb{Z}, r = \frac{a_1}{b_1}, b_1 = p^{k_1}, k_1 \in \mathbb{Z}^+ \cup \{0\}$ $\exists\, a_2, b_2 \in \mathbb{Z}, s = \frac{a_2}{b_2}, b_2 = p^{k_2}, k_2 \in \mathbb{Z}^+ \cup \{0\}$
$r + s = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \in \mathbb{Q}$
$a_1 b_2 + a_2 b_1 \in \mathbb{Z}$
$b_1 \neq 0$ and $b_2 \neq 0$ so $b_1 b_2 \neq 0$
$b_1 b_2 = p^{k_1} p^{k_2} = p^{k_1 + k_2}$
But $k_1 + k_2 \in \mathbb{Z}^+ \cup \{0\}$
$\therefore r + s \in R^p$ and $\langle R^p, + \rangle$ is closed.

$\langle \mathbb{Q}, + \rangle$ is associative, so $\langle R^p, + \rangle$ is associative.

$p^0 = 1$, so $\frac{0}{1} \in R^p$
Assume $r = \frac{a}{b} \in R_p$
$\frac{0}{1} + r = \frac{0}{1} + \frac{a}{b} = \frac{0b + 1a}{1b} = \frac{a}{b} = r$
$r + \frac{0}{1} = \frac{a}{b} + \frac{0}{1} = \frac{1a + 0b}{1b} = \frac{a}{b} = r$
$\therefore \frac{0}{1}$ is a two-sided identity for R_p.

Assume $r = \frac{a}{b} \in R_p$
$-r = -\frac{a}{b} = \frac{(-a)}{b} \in R_p$
$-r + r = -\frac{a}{b} + \frac{a}{b} = 0 = \frac{0}{1}$
$r + (-r) = \frac{a}{b} - \frac{a}{b} = 0 = \frac{0}{1}$
$\therefore -r$ is a two-sided inverse for r.

$\langle \mathbb{Q}, + \rangle$ is commutative, so $\langle R^p, + \rangle$ is commutative.

$\therefore \langle R^p, + \rangle$ is an abelian group.

1.1.12

Let G be a group such that $\forall\, a, b \in G, \exists\, r \in \mathbb{Z}^+, bab^{-1} = a^r$.

Prove: $\forall\, a, b \in G, \forall\, n \in \mathbb{Z}^+, b^n a b^{-n} = a^{r^n}$

Proof by induction on n

Base: $n = 1$

$$b^1 a b^{-1} = bab^{-1} = a^r = a^{r^1}$$

Assume $\forall\, a, b \in G, \forall\, n \in \mathbb{Z}^+, b^n a b^{-n} = a^{r^n}$

Consider $(n+1)$

$$\begin{aligned} b^{n+1}ab^{-(n+1)} &= b(b^n ab^{-n})b^{-1} \\ &= b(a^{r^n})b^{-1} \\ &= b(b^{-1}ba)^{r^n}b^{-1} \\ &= (bb^{-1})(bab^{-1})^{r^n} \\ &= e(a^r)^{r^n} \\ &= (a^r)^{r^n} \\ &= a^{rr^n} \\ &= a^{r^{(n+1)}} \end{aligned}$$

1.1.13

Let G be a group. Prove: $(\forall\, a \in G, a^2 = e) \implies G$ is abelian.

Assume $\forall\, a \in G, a^2 = e$
Assume $a, b \in G$
$ab \in G$
$(ab)^2 = e$
$(ab)(ab) = e$
$a(ab)(ab)b = aeb$
$(aa)(ba)(bb) = ab$
$ebae = ab$
$ba = ab$
$\therefore G$ is abelian.

1.1.15

Let G be a semigroup such that the left and right cancellation rules hold.

a) Prove: G is finite $\implies G$ is a group.

   Assume G is finite
   Let $|G| = n$
   Assume $a \in G$
   By closure of the binary operation, $\forall\, m \in \mathbb{Z}^+, a^m \in G$
   Let $S = \{a^m \mid 1 \leq m \leq n+1\}$
   $S \subseteq G$, but $|S| = n+1 > n = |G|$
   Thus, S must have duplicates
   Assume $a^j = a^k, j < k$

Case 1: $j = 1$

$a = a^k = a^{k-1+1} = a^{k-j+1}$

Case 2: $j > 1$

G is associative, and thus so is S
$aa^{j-1} = a^{k-j+1}a^{j-1}$
So, by right cancellation, $a = a^{k-j+1}$

Thus, combining the two cases, $a = a^{k-j+1} \in S$ and also in G

G is a semigroup and is thus associative.

Now, assume $b \in G$
$ba = ba^{k-j+1} = ba^{k-j}a$
By right cancellation, $b = ba^{k-j}$
$ab = a^{k-j+1}b = aa^{k-j}b$
By left cancellation, $b = a^{k-j}b$
$\therefore a^{k-j}$ is a two-sided identity for G.

Remember that a was selected as any arbitrary element in G
Since $e \in G$, $e = a^0$ is defined
$a = a^{k-j+1}$
$ea = a^{k-j-1}aa$
By right cancellation, $e = a^{k-j-1}a$
$ae = aaa^{k-j-1}$
By left cancellation, $e = aa^{k-j-1}$
$\therefore a^{k-j-1}$ is a two-sided inverse for a.

$\therefore G$ is a group.

b) If G is infinite, then the implication does not hold. As a counter-example, consider $\langle Z^+, + \rangle$. It is a semigroup and the cancellation rules hold; however, there is no identity or inverses and thus it is not a group.