Abstract Algebra I HW1

Chengyu Hsieh, B13201053

1) From now on, for simplicity's sake, we let $f_i f_j$ denote $f_i(f_j(x))$.

   (a) By Calculation we find that f_2, f_3, f_6 satisfy the required property.

   (b) Note that $(12)(12), (13)(13), (23)(23)$ all equal to (1). Also see that $f_6 = f_2 f_5$, $f_3 = f_2 f_5 f_5$, $f_4 = f_5 f_5$. Furthermore, $(13) = (12)(123)(123), (23) = (12)(123), (132) = (123)(123)$. Our correspondence should have the property that if f_i corresponds to x, f_j corresponds to y, then $f_i f_j$ corresponds to xy. By this rule, we let f_2 correspond to (12), and f_5 correspond to (123). We may check via calculation that this satisfy the mentioned rule. Hence one correspondence is for f_2 to correspond to (12), f_6 to correspond to (13) and f_3 to correspond to (23).

   (c) $f_2 f_6 = f_4$, $f_6 f_2 = f_5$, $f_2 f_3 = f_5$, $f_3 f_2 = f_4$, $f_3 f_6 = f_5$, $f_6 f_3 = f_4$. Hence for two distinct f_i, f_j obtained in (a), we have $f_i \neq f_j$. In (b) we already have that if f_i corresponds to x, f_j corresponds to y, then $f_i f_j$ corresponds to xy. It follows that for $x, y \in \{(12), (23), (13)\}, x \neq y$, we have $xy \neq yx$.

   (d) f_5 corresponds to (123), and f_4 corresponds to (132).

2) We assume 3) is already proven. By Claim 1, we will list the elements that are coprime with n. Since the calculations are too trivial and repetitive, we do not show it here.

   (a) $\{1, 2, 3, 4\}$

   (b) $\{1, 5\}$

   (c) $\{1, 3, 5, 7\}$

   (d) $\{1, 7, 13\}$

   (e) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

3) (a) **Necessity:** Assume that $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then by definition, there exists $y \in \mathbb{Z}/n\mathbb{Z}$ such that $xy \equiv 1 \mod n$. Hence $xy = \beta n + 1$ for some $\beta \in \mathbb{Z}$. If we let $a = y$ and $b = -\beta$ then $ax + bn = 1$.

   Sufficiency: Assume that there exists integers a, b such that $ax + bn = 1$. Let $a = \alpha + \beta n$, $0 \leq \alpha \leq n - 1$, $\alpha, \beta \in \mathbb{Z}$.
   Thus $0 \leq \alpha \leq n - 1$ and is in $\mathbb{Z}/n\mathbb{Z}$.

$$
\begin{aligned}
&\alpha x + (b + \beta)n = 1 \\
&\Rightarrow x\alpha = -(\beta + b)n + 1 \\
&\Rightarrow x\alpha \equiv 1 \mod n
\end{aligned}
$$

   By our definition we have $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(b)

Claim 1. Let $a, b \in \mathbb{Z}$, $a, b > 0$. If $\exists c, d \in \mathbb{Z}$ such that $ca + db = 1$, then$(a, b) = 1$.

Proof. Suppose $(a, b) = k > 1$. Let $a = k\alpha$, $b = k\beta$. Let c, d be integers such that $ca + db = 1$. Subsitute in $k\alpha$ and $k\beta$ we obtain '

$$k(c\alpha + d\beta) = 1$$

Since k and $c\alpha + d\beta$ are integers, we have $(k = 1 \wedge c\alpha + d\beta = 1) \vee (k = -1 \wedge c\alpha + d\beta = -1)$. But we assumed that $k > 1$ and so we arrived at an contradiction. Hence $(a, b) = 1$.

Claim 2. Let $a, b \in \mathbb{Z}$, $a, b > 0$. If $(a, b) = m$, then exists $c, d \in \mathbb{Z}$ such that $ca + db = m$.

Proof. First note that if $d|a \wedge d|b$, then $d|m$. Now let $M = \{ca+db|c, d \in \mathbb{Z}\}$. $1a+0b = a > 0$, so M has positive integers. Let $M^+ = \{ca + db > 0|c, d \in \mathbb{Z}\}$, which is non empty. Clearly $\min M^+$ exist. Let $m' = \min M^+$. Then $m' = c'a + d'b$ for some $c', d' \in \mathbb{Z}$. Now for any $x = ca + db \in M$, let $x = m'q + r$ with $0 \leq r < m'$.

$$r = x - m'q = (c - c'q)a + (d - d'b)b \in M$$

Since we have $0 \leq r < m'$, we have $r = 0$. (Otherwise $m' \neq \min(M^+)$).) Therefore $m'|x \forall x \in M$. Note that $a, b \in M \Rightarrow m'|a \wedge m'|b$. Also, for any d such that $d|a \wedge d|b$ we have $d|c'a + d'b$, so $d|m'$. Hence $m' = (a, b) = m$. We conclude that $\exists c, d \in \mathbb{Z}$ such that $ca + db = m$.

Sufficiency:
Suppose n is prime. Then for any $x \neq 0 \in \mathbb{Z}/n\mathbb{Z}$ we have $(x, n) = 1$. Hence by Claim 2, there exists $c, d \in \mathbb{Z}$ such that $cx + dn = 1$. Then by (a), we have $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Since $(\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ has $n-1$ elements and every element of $(\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ is in $(\mathbb{Z}/n\mathbb{Z})^\times$, we conclude that $(\mathbb{Z}/n\mathbb{Z})^\times$ has $n - 1$ elements.
Necessity:
Suppose $(\mathbb{Z}/n\mathbb{Z})^\times$ has $n - 1$ elements. Clearly, $(\mathbb{Z}/n\mathbb{Z})^\times = \{1, 2, ..., n - 1\}$. By Claim 1, we have $(x, n) = 1$ for every x such that $1 \leq x \leq n - 1$. Therefore n is prime.

4) (a) Suppose e, e' are identity elements of G. Since $e * x = x \forall x \in G$,

$$e * e' = e'$$

Since $x * e' = x \forall x \in G$,

$$e * e' = e$$

Therefore $e = e'$. We conclude that the identity element is unique.

Now for an element $x \in G$, suppose that b, c are both the inverse of x.

$$b = b * e = b * (x * c) = (b * x) * c = e * c = c$$

Hence the inverse of an element is unique.

(b) In the following discussion we let e denote the identity element of G. Also, the fact that $ex = xe$ for $x \in G$ is very clear and will not be checked from now on.

Case $|G| = 1$:
Let $G = \{e\}$. Trivial.
Case $|G| = 2$:
Let $G = \{e, a\}$. Trivial.
The cases from now on are not so trivial, so we introduce and prove the following claims:

Claim 3. For a fixed $x \in G$ we have $xy_1 \neq xy_2$ for $y_1, y_2 \in G$, $y_1 \neq y_2$.

Proof. Assume otherwise. Then $y_1 = x^{-1}xy_1 = x^{-1}xy_2 = y_2$, contradicting our assumption.

Claim 4. Let $x, y \in G, x, y \neq e$. Then $xy \neq x$ and $xy \neq y$.

Proof. Assume $xy = x$. Then $y = x^{-1}xy = x^{-1}x = e$, giving a contradiction. Hence $xy \neq x$. Assuming $xy = y$ gives a similar contradiction.

Case $|G| = 3$:
Let $G = \{e, a, b\}$. By Claim 3, $a^2 \neq a$, so $a^2 = a$ or b.
If $a^2 = e$, by Claim 3 we have $ab = b$ which contradict Claim 4.
Hence $a^2 = b$. By Claim 3 we have $ba = e = ab$. By Claim 3 again we have $b^2 = a$. Hence $ab = ba$.
Case $|G| = 4$:
By Claim 3, $a^2 \neq a$.
If $a^2 = e$:
By Claim 3, $ab, ba \neq a, e$. By Claim 4, $ab, ba \neq b$. Hence $ab = c = ba$. By Claim 3, $ac = b = ca$. Note that $b^2 \neq c$ by Claim 3.
If $b^2 = e$:
By Claim 3, $bc = a = cb$, $c^2 = e$. In this case, $ab = ba, bc = cb, ac = ca$.
If $b^2 = a$:
By Claim 3, $bc = e = cb$, $c^2 = a$. In this case, $ab = ba, bc = cb, ac = ca$.
If $a^2 = b$:
By Claim 4, $ac = e = ca$. By Claim 3, $ab = c = ba$.
If $b^2 = e$:
By Claim 3, $bc = a = cb$, $c^2 = e$. In this case, $ab = ba, bc = cb, ac = ca$.
If $b^2 = a$:
By Claim 3, $bc = e = cb$, $c^2 = a$. In this case, $ab = ba, bc = cb, ac = ca$.
For $a^2 = c$, this case is analogus to case $a^2 = b$
We conclude that if G has at most elements, G must be abelian.

(c) For any $x, y \in G$, note that $xxyy = ee = e$. Also, $(xy)(xy) = e$. Then, $xxyy = xyxy$ and so $xy = yx$.