Math40003 Linear Algebra and Groups
Term 2 Unseen 4B Groups (Week 7)

Recall the following lemma and fact that you may want to use for some of the questions.

Lemma 1 (Corollary 3.2.1 (?) from Introduction to University Mathematics). *Let $a, b \in \mathbb{Z}$. If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.*

Fact 1 (The Pigeonhole Principle). *Let A be a finite set, and let $f : A \to A$ be a function on A. Then f is injective if and only if it is surjective.*

1. Let us define a new algebraic structure, *group**, to be a set A, with an associative binary operation, denoted by $\cdot$, and an element $e \in A$ satisfying:

   - $\forall a \in A : a \cdot e = a$.
   - $\forall a \in A : \exists a' \in A$, such that $a \cdot a' = e$.

   Prove that this new algebraic structure, *group**, gives the classical group structure. In other words, prove that if $(A, \cdot)$ is a group*, then it is a group.

   It suffices to show:

   (a) $\forall a \in A : e \cdot a = a$**.**

   (b) $\forall a \in A : \exists a' \in A$**, such that** $a' \cdot a = a \cdot a' = e$**.**

   For Item 1b, let $a \in A$**, let** $a' \in A$ **such that** $a \cdot a' = e$ **and let** $a'' \in A$ **such that** $a' \cdot a'' = e$**, as promised from the definition of group*. Then**

   $$a' \cdot a = a' \cdot (a \cdot e) = a' \cdot (a \cdot a') \cdot a'' = (a' \cdot e) \cdot a'' = a' \cdot a'' = e.$$

   For Item 1a, let $a \in A$**. Then**

   $$e \cdot a = (a \cdot a') \cdot a = a \cdot (a' \cdot a) = a \cdot e = a.$$

2. A *monoid* is a set A with an associative binary operation $\circ$ and an element $e \in A$ such that

   $$\forall a \in A : a \circ e = e \circ a = a.$$

   Let $(A, \circ)$ be a monoid, and let $A^\times := \{ a \in A | \exists b \in A : a \circ b = b \circ a = e \}$. Prove that $(A^\times, \circ)$ is a group.

   Clearly $\circ$ is associative on $A^\times$ and $e \in A^\times$. It remains to show that for all $a \in A^\times$, there is some $b \in A^\times$ such that $a \circ b = b \circ a = e$. Such b exists in A, so it is only left to show it is in $A^\times$, but this follows from the definition.

   Closedness: let $a_1, a_2 \in A^\times$**, and let** $b_1, b_2 \in A^\times$ **such that** $a_1 \circ b_1 = a_2 \circ b_2 = e$**. Then** $a_1 \circ a_2 \circ b_2 \circ b_1 = a_1 \circ e \circ b_1 = a_1 \circ b_1 = e$**.**

3. We recall the definition of $\mathbb{Z}/n\mathbb{Z}$ (Sometimes denoted $\mathbb{Z}_n$). For $a, b \in \mathbb{Z}$, denote $a \equiv b \mod n$ if $n|a-b$. This is an equivalence relation with n equivalence classes. The set of equivalence classes is denoted

$$\mathbb{Z}/n\mathbb{Z} = \{ [0], [1], \dots, [n-1] \} .$$

The operations $+, \cdot$ on $\mathbb{Z}/n\mathbb{Z}$ are defined as follows: $[a]+[b] = [a+b]$; $[a]\cdot[b] = [a\cdot b]$.

(a) Prove $(\mathbb{Z}/n\mathbb{Z}, +)$ is an Abelian group.

(b) $\cdot$ is associative and commutative on $\mathbb{Z}/n\mathbb{Z}$, but $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is not a group.

4. Let $(\mathbb{Z}/n\mathbb{Z})^\times := \{ [a] \in \mathbb{Z}/n\mathbb{Z} | \exists [b] \in \mathbb{Z}/n\mathbb{Z} : [a] \cdot [b] = [1] \}$.

(a) Prove $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ is an Abelian group.
Questions 2 and 3b.

(b) Show that for $[a] \in (\mathbb{Z}/n\mathbb{Z})$ the following are equivalent:

(i) $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(ii) $\forall [c] \in (\mathbb{Z}/n\mathbb{Z})$: if $[a] \cdot [c] = [0]$ then $[c] = [0]$.

(iii) $\gcd(a, n) = 1$.

(i)$\Longrightarrow$(ii) **Let $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then there is some $[b] \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $[a] \cdot [b] = [1]$. If there is some $[c] \in (\mathbb{Z}/n\mathbb{Z}) \setminus \{ [0] \}$ such that $[a] \cdot [c] = [0]$. Then $ac = nk$ and $ab - 1 = nl$. So $nkb - c = cab - c = c(ab - 1) = cnl$. Therefore, $[c] = [0]$.**

(ii)$\Longrightarrow$(iii) **Assume $\gcd(a, n) = d > 1$. Then there are $0 < a' < a$ and $0 < n' < n$ such that $a = a'd$ and $n = n'd$. So $an' = a'n'd = a'n$ So $[a] \cdot [n'] = [0]$, but $0 < n' < n$, so $[n'] \neq [0]$.**

(ii)$\Longleftarrow$(iii) **Assume there is some $[c] \in (\mathbb{Z}/n\mathbb{Z})$ such that $[c] \neq [0]$ and $[a] \cdot [c] = [0]$. Then $ac = nk$ for some $k \in \mathbb{Z}$. Therefore, $n|ac$. If $\gcd(a, n) = 1$, then $n|c$, contradicting $[c] \neq [0]$.**

(i)$\Longleftarrow$(ii) **Assume there is no $[c] \in (\mathbb{Z}/n\mathbb{Z})$ such that $[c] \neq [0]$ and $[a]\cdot[c] = [0]$. Then we have a map $f : (\mathbb{Z}/n\mathbb{Z}) \setminus \{ [0] \} \to (\mathbb{Z}/n\mathbb{Z}) \setminus \{ [0] \}$ defined by $f(x) = [a] \cdot x$. Furthermore, by Lemma 1, f is injective: if $[a \cdot b_1] = f([b_1]) = f([b_2]) = [a \cdot b_2]$, then $[b_1 - b_2] = [0]$, therefore, $[b_1] = [b_2]$. By the Pigeonhole Principle, f is also surjective, therefore, since $[1] \neq [0]$ there is some $[b] \in (\mathbb{Z}/n\mathbb{Z}) \setminus \{ [0] \}$ such that $[a] \cdot [b] = [1]$.**

(c) Let $a, b, x, y \in \mathbb{Z}$ such that $ax + by = 1$, then $\gcd(a, b) = 1$.

(d) Find the size of the sets $(\mathbb{Z}/8\mathbb{Z})^\times$ and $(\mathbb{Z}/9\mathbb{Z})^\times$. Try generalizing your findings.
For p prime: $(\mathbb{Z}/p^r\mathbb{Z})^\times = p^r - p^{r-1}$. The elements in $\mathbb{Z}/p^r\mathbb{Z}$ that are not in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ are exactly $p\mathbb{Z}/p^r\mathbb{Z}$.