Imperial College London
Department of Mathematics

Unseen 5

MATH40003 Linear Algebra and Groups — Term 2, 2022/23

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

Lemma 1. *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.

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 $A^\times := \{a \in A \mid \exists b \in A : a \circ b = b \circ a = e\}$. Prove that $(A^\times, \circ)$ is a group.

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
$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$
   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 $(\mathbb{Z}/n\mathbb{Z})^\times := \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \exists [b] \in \mathbb{Z}/n\mathbb{Z} : [a] \cdot [b] = [1]\}$.

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

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

(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.