Math 3140 - Assignment 2

Due September 4, 2026

(1) (a) Show that $\{1,2,3\}$ under multiplication modulo 4 is not a group.
(b) Show that $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is a group.

Solution: (a) E.g. $2 \cdot 2 = 0 \not\in \{1,2,3\}$. So multiplication modulo 4 is not an operation on $\{1,2,3\}$.
(b) $\mathbb{Z}_5 \setminus \{0\}$ is closed under multiplication since 5 is prime.
Associativity is inherited from the multiplication on $\mathbb{Z}$.
1 is the identity.
Every element has a multiplicative inverse $1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$.

(2) Compute the following multiplicative inverses in $\mathbb{Z}_n$ if possible:
(a) $[12]^{-1}$ in $\mathbb{Z}_{35}$
(b) $[14]^{-1}$ in $\mathbb{Z}_{35}$
Hint: Use the Euclidean Algorithm to compute Bezout's coefficients.

Solution: In $\mathbb{Z}_{35}$ we get $[12]^{-1} = [3]$ but $[14]^{-1}$ does not exist since $\gcd(14,35) = 7 \neq 1$.

(3) Let $n \geq 2$ and a be integers. Show that $ax \mod n = 1$ has a solution iff $\gcd(a,n) = 1$.

Solution: $\Rightarrow$ Assume $ax \mod n = 1$ has a solution $x \in \mathbb{Z}$. That means $ax - 1$ is a multiple of n, say $ax - 1 = ny$ for $y \in \mathbb{Z}$. So

$$ax - ny = 1$$

Since $\gcd(a,n)$ divides the lefthand side, it follows that $\gcd(a,n) = 1$.
$\Leftarrow$ Assume $\gcd(a,n) = 1$. By Bezout's identity there exist $x, y \in \mathbb{Z}$ such that

$$ax + ny = \gcd(a,n) = 1.$$

Then $ax \equiv_n 1$ as required.

(4) For $n \in \mathbb{N}$, let $\mathbb{Z}_n^*$ denote the set of elements in $\mathbb{Z}_n$ that have a multiplicative inverse. Show that $(\mathbb{Z}_n^*, \cdot)$ is a group.

Hint: Don't forget to show that $\cdot$ is an operation on $\mathbb{Z}_n^*$, i.e., that the product of invertible elements is invertible again.

Solution: First check that $\cdot, ^{-1}, 1$ are operations on $\mathbb{Z}_n^*$.

(a) $[1] \in \mathbb{Z}_n^*$ since $[1]$ is its own multiplicative inverse.

(b) $\mathbb{Z}_n^*$ is closed under multiplication: Let $a, b \in \mathbb{Z}_n^*$ have multiplicative inverses a^{-1}, b^{-1}, respectively. Then ab has the inverse $b^{-1}a^{-1}$, hence is in $\mathbb{Z}_n^*$ as well.

(c) $\mathbb{Z}_n^*$ is closed under $^{-1}$: Let $a \in \mathbb{Z}_n^*$ have a multiplicative inverse a^{-1}. Then a is the inverse of a^{-1}, hence a^{-1} is in $\mathbb{Z}_n^*$ as well.

Next check that $(\mathbb{Z}_n^*, \cdot, ^{-1}, 1)$ satisfies the group axioms:

(d) $\mathbb{Z}_n^* \neq \emptyset$ since it contains the identity $[1]$ by (a).

(e) $(\mathbb{Z}_n^*, \cdot)$ is associative because $(\mathbb{Z}, \cdot)$ is (mentioned in class).

(f) For every $[a] \in \mathbb{Z}_n^*$ we have $[a][1] = [1][a] = [a]$ by the definition of multiplication on $\mathbb{Z}_n$.

(g) For every $a \in \mathbb{Z}_n^*$ we have $aa^{-1} = a^{-1}a = 1$ since a^{-1} is defined as the multiplicative inverse of a.

(5) Let A, B be subgroups of a group $(G, \cdot)$. Show that $A \cap B$ is a subgroup as well.

Solution: (a) $A \cap B \neq \emptyset$: Note $1 \in A \cap B$ since A, B are subgroups hence both contain 1.

(b) $A \cap B$ is closed under multiplication: Let $x, y \in A \cap B$. Then $xy \in A$ and $xy \in B$ since both are subgroups. So $xy \in A \cap B$.

(c) $A \cap B$ is closed under inverses: as above.