**Math 561/661** **Fall 2023**
**Homework 3** **Drew Armstrong**

---

**1. Working with Lattice Axioms.** Let $(P, \leq, \wedge, \vee)$ be a lattice. For all $a, b \in P$ prove that

$$a \leq b \iff a = a \wedge b.$$

**2. Divisibility is a Partial Order.** Consider the set $\mathbb{N} = \{0, 1, 2, \ldots\}$ together with the relation of *divisibility*:

$$a|b \iff \text{there exists some } k \in \mathbb{Z} \text{ such that } ak = b.$$

(a) For all $a \in \mathbb{N}$ prove that $a|a$.
(b) For all $a, b \in \mathbb{N}$ prove that $a|b$ and $b|a$ imply $a = b$. [Hint: For any integers $c, d \in \mathbb{Z}$ you can assume that $cd = 0$ implies $c = 0$ or $d = 0$.]
(c) For all $a, b, c \in \mathbb{Z}$ prove that $a|b$ and $b|c$ imply $a|c$.

**3. The Group of Units Mod $n$.** Consider the ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, 0, 1)$. We say that $u \in \mathbb{Z}/n\mathbb{Z}$ is a *unit* if there exist some $x \in \mathbb{Z}/n\mathbb{Z}$ such that $ux \equiv 1 \bmod n$. We denote the *multiplicative group of units* by $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot, 1)$.

(a) Prove that $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$. [Hint: We proved in class that $a\mathbb{Z} + n\mathbb{Z} = \gcd(a, n)\mathbb{Z}$ for all $a, n \in \mathbb{Z}$. In particular, this implies that there exist $x, y \in \mathbb{Z}$ such that $ax + ny = \gcd(a, n)$.]
(b) Write down the full group tables of $(\mathbb{Z}/10\mathbb{Z})^\times$ and $(\mathbb{Z}/12\mathbb{Z})^\times$. Each of these groups has size 4. Prove that they are not isomorphic.

**4. Order of a Power.** Let $(G, *, \varepsilon)$ be a group and let $g \in G$ be an element of order $n \geq 1$.

(a) For any integer $k \in \mathbb{Z}$, let $d = \gcd(k, n)$. Show that $\langle g^k \rangle = \langle g^d \rangle$. [Hint: It suffices to show that $g^k$ is a power of $g^d$ and that $g^d$ is a power of $g^k$. For the second statement you should use Bézout's identity: $k\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$.]
(b) For any positive divisor $d|n$ show that $g^d$ has order $n/d$. [Hint: Let $m = n/d$. You need to show that $(g^d)^m = \varepsilon$ and that the elements $\varepsilon, (g^d)^1, \ldots, (g^d)^{m-1}$ are distinct.]
(c) Combine (a) and (b) to show that for any $k \in \mathbb{Z}$ the element $g^k$ has order $n/\gcd(n, k)$.

**5. The Euler-Fermat-Lagrange Theorem.** Let $(G, \cdot, 1)$ be an abelian group and let $a \in G$ be any element. Define the function $\tau_a : G \to G$ by $\tau_a(g) := ag$.

(a) Prove that $\tau_a : G \to G$ is a bijection.
(b) If the group $G$ is **finite**, prove that $a^{\#G} = 1$. [Hint: Suppose that $\#G = n$ and list the elements as $G = \{g_1, g_2, \ldots, g_n\}$. Explain why $g_1 g_2 \cdots g_n = \tau_a(g_1)\tau_a(g_2)\cdots\tau_a(g_n)$. Rearrange the elements and then cancel.]
(c) If $p$ is prime and $a \nmid p$, show that the result from part (b) implies

$$a^{p-1} \equiv 1 \bmod p\ .$$

[Hint: Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$. See Problem 3.]

**6. Image and Preimage.** Let $\varphi : (G, *, \varepsilon_G) \to (H, \bullet, \varepsilon_H)$ be a group homomorphism. For any sub**set** $S \subseteq G$ we define the *image* set $\varphi[S] \subseteq H$ by

$$\varphi[S] := \{h \in H : \text{there exists } g \in S \text{ such that } \varphi(g) = h\}$$

and for any sub**set** $T \subseteq H$ we define the *preimage* set $\varphi^{-1}[T] \subseteq G$ by

$$\varphi^{-1}[T] := \{g \in G : \varphi(g) \in T\}.$$

Remark: We do not assume that the inverse function $\varphi^{-1} : H \to G$ exists. It exists if and only if for each element $h \in H$ the preimage set $\varphi^{-1}[\{h\}]$ consists of exactly one element.

(a) For any sub**sets** $S \subseteq G$ and $T \subseteq G$, prove that

$$S \subseteq \varphi^{-1}[T] \quad \Longleftrightarrow \quad \varphi[S] \subseteq T.$$

(b) If $S \subseteq G$ is a sub**group**, prove that $\varphi[S] \subseteq H$ is a sub**group**.

(c) If $T \subseteq H$ is a sub**group**, prove that $\varphi^{-1}[T] \subseteq G$ is a sub**group**.