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

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

By definition, the element $a \wedge b$ satisfies (and is uniquely determined by) three properties:

- $a \wedge b \leq a$,
- $a \wedge b \leq b$,
- if $c \leq a$ and $c \leq b$ then $c \leq a \wedge b$.

First suppose that $a = a \wedge b$. Then since $a \wedge b \leq b$ we have $a \leq b$. Conversely, **suppose that** $a \leq b$. In this case we wish to show that $a = a \wedge b$. If we can show that $a \leq a \wedge b$ and $a \wedge b \leq a$ then we will be done by using the anti-symmetry axiom of "$\leq$". And we already know that $a \wedge b \leq a$ from the definition of "$\wedge$".

It only remains to show that $a \leq a \wedge b$. Since we have $a \leq a$ (by definition) and $a \leq b$ (by assumption) we see that a is a lower bound of a and b, hence it follows from the "greatest lower bound" axiom that $a \leq a \wedge b$. $\square$

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 $a, b, c \in \mathbb{N}$ prove that $a|b$ and $b|c$ imply $a|c$.

(a): For all $a \in \mathbb{N}$ we have $a \cdot 1 = a$ and hence $a|a$.

(b): Suppose that $a, b \in \mathbb{N}$ satisfy $a|b$ and $b|a$. In other words, suppose we have $ak = b$ and $b\ell = a$ for some $k, \ell \in \mathbb{Z}$. If one of a or b is zero then the other must be as well, hence $a = 0 = b$. So let us assume that $a \neq 0$ and $b \neq 0$. Then we have

$$\begin{aligned} a &= b\ell \\ a &= ak\ell \\ a(1 - k\ell) &= 0 \\ 1 - k\ell &\overset{*}{=} 0 \\ 1 &= k\ell. \end{aligned}$$

Step $*$ follows from the fact that $a \neq 0$ and the cancellation property of the integers.[1] This last equation has only two solutions: $k = \ell = 1$ or $k = \ell = -1$. The solution $k = \ell = -1$ is impossible because a and b are both positive, hence $k = \ell = 1$ and we conclude that $a = b\ell = b \cdot 1 = b$.

[1] Technically, the integers satisfy the property that $c \neq 0$ and $d \neq 0$ implies $cd \neq 0$. A general commutative ring satisfying this condition is called an *integral domain* (i.e., a place in which to do arithmetic that is similar to the integers).

(c): Suppose that $a, b, c \in \mathbb{N}$ satisfy $a|b$ and $b|c$. This means that there exist $k, \ell \in \mathbb{Z}$ satisfying $kb = c$ and $\ell a = b$. It follows that $(k\ell)a = c$ and hence $a|c$.

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.

(a): If $a \in \mathbb{Z}/n\mathbb{Z}$ is a unit then we have $ax \equiv 1 \bmod n$ for some integer $x \in \mathbb{Z}$. By definition this means that $1 - ax = ny$ for some $y \in \mathbb{Z}$, and hence $ax + ny = 1$. I claim that this implies $\gcd(a, n) = 1$. Indeed, let $d = \gcd(a, n)$. Since d is a common divisor of a and n we have $a = da'$ and $n = dn'$ for some $a', n' \in \mathbb{Z}$, and hence

$$1 = ax + ny = da'x + dn'y = d(a'x + n'y),$$

It follows that $d = 1$.[2]

Conversely, suppose that $\gcd(a, n) = 1$. We proved in class that $a\mathbb{Z} + n\mathbb{Z} = \gcd(a, b)\mathbb{Z}$, so in this case we have $a\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Since $1 \in a\mathbb{Z} + n\mathbb{Z}$ we have $1 = ax + ny$ for some $x, y \in \mathbb{Z}$. It follows that $n|(1 - ax)$ and hence $ax \equiv 1 \bmod n$. In other words, a is a unit of $\mathbb{Z}/n\mathbb{Z}$.

[Remark: Our proof from class that $a\mathbb{Z} + n\mathbb{Z} = \gcd(a, n)\mathbb{Z}$ was indirect. The Euclidean algorithm can be used to compute specific integers $x, y \in \mathbb{Z}$ satisfying $ax + ny = \gcd(a, n)$.]

(b): Here are the group tables of $(\mathbb{Z}/10\mathbb{Z})^\times$ and $(\mathbb{Z}/12\mathbb{Z})^\times$:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

The group $(\mathbb{Z}/10\mathbb{Z})^\times$ has 2 elements of order, while $(\mathbb{Z}/12\mathbb{Z})^\times$ has 4 elements of order two; hence they are not isomorphic. To be more specific, $(\mathbb{Z}/10\mathbb{Z})^\times$ is cyclic, hence is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. The only other group of size 4 is the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, hence $(\mathbb{Z}/12\mathbb{Z})^\times$ must be isomorphic to this.

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 $n/\gcd(n, k)$.

[2] In general, if $a|b$ and $b \neq 0$ then $|a| \leq |b|$. Proof: Suppose that $b = ak$. Since $b \neq 0$ we have $a \neq 0$ and $k \neq 0$, so that $|a| \geq 1$ and $|k| \geq 1$, because these are whole numbers. Multiply both sides of the inequality $1 \leq |k|$ by $|a|$ to get $|a| \leq |a||k| = |ak| = |b|$. This proof will look slightly different depending on what axiom system you are using for the integers.

(a): Let $g \in G$ be an element of a group, with $\#\langle g \rangle = n$, and let $d = \gcd(k, n)$. In this case we will prove that $\langle g^k \rangle = \langle g^d \rangle$.

In order to prove that $\langle g^k \rangle \subseteq \langle g^d \rangle$ it suffices to show that $g^k \in \langle g^d \rangle$. Note that $d = \gcd(k, n)$ is a divisor of k, hence $k = dd'$ for some $d' \in \mathbb{Z}$. Then we have

$$g^k = g^{dd'} = (g^d)^{d'} \in \langle g^d \rangle.$$

Conversely, in order to prove that $\langle g^d \rangle \subseteq \langle g^k \rangle$, it suffices to show that $g^d \in \langle g^k \rangle$. For this we use Bézout's identity to write $d = kx + ny$ for some $x, y \in \mathbb{Z}$. Then we have

$$g^d = g^{kx+ny} = (g^k)^x * (g^n)^y = (g^k)^x * \varepsilon^y = (g^k)^x \in \langle g^k \rangle.$$

(b): For any positive divisor $d|n$, let $n = dm$. Then we have

$$(g^d)^m = g^n = \varepsilon.$$

If we can show that the elements $\varepsilon, g^d, (g^d)^2, \ldots, (g^d)^{m-1}$ are distinct then it will follow that $\#\langle g^d \rangle = m = n/d$. To show this, we assume for contradiction that $(g^d)^k = (g^d)^\ell$ for some $0 \leq k < \ell < m$. Multiplying both sides by $(g^d)^{-k}$ gives $g^{d(\ell-k)} = \varepsilon$, where $1 \leq \ell - k < m$. Multiplying this inequality by d gives $1 \leq d \leq d(\ell - k) < dm = n$. But we showed on the previous homework that if $\#\langle g \rangle = n$ then n is the smallest positive integer satisfying $g^n = \varepsilon$. Hence we have a contradiction.

(c): Let $\#\langle g \rangle = n$ and let $d = \gcd(k, n)$, where k is any integer. From part (a) we have $\langle g^k \rangle = \langle g^d \rangle$. Then from part (b) we have

$$\#\langle g^k \rangle = \#\langle g^d \rangle = n/d = n/\gcd(k, n).$$

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.]

(a): For any $a \in G$ we define the "translation function" $\tau_a : G \to G$ by $\tau_a(g) := ag$. I claim that this function is invertible, with inverse $\tau_{a^{-1}}$. Indeed, for any $g \in G$ we have $\tau_{a^{-1}}(\tau_a(g)) = a^{-1}ag = g$ and $\tau_a(\tau_{a^{-1}}(g)) = aa^{-1}g = g$, which shows that $\tau_a \circ \tau_{a^{-1}}$ and $\tau_{a^{-1}} \circ \tau_a$ are the identity function.

(b): Let $\#G = n$ and denote the elements of G as $g_1, g_2, \ldots, g_n$. For any $a \in G$, we know from part (a) that the elements $ag_1, ag_2, \ldots, ag_n$ are distinct, hence this is just a rearrangement of the group elements. Let $h = g_1 g_2 \cdots g_n$ be the product of all the group elements. Then we also have

$$h = (ag_1)(ag_2)\cdots(ag_n) = a^n g_1 g_2 \cdots g_n = a^n h.$$

Finally, multiplying both sides by the inverse h^{-1} gives $a^n = 1$ as desired.

(c): There is not much to "do" here. From Problem 3 we know that $\#(\mathbb{Z}/p\mathbb{Z})^\times = p - 1$. If $G = (\mathbb{Z}/p\mathbb{Z})^\times$ then part (b) tells us that every element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfies "$a^{p-1} = 1$". Now we translate these abstract statements into the language of integers: Given any integer $a \in \mathbb{Z}$ such that $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, i.e., such that $\gcd(a, p) = 1$, i.e., such that $p \nmid a$, we have "$a^{p-1} = 1$" in the group $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e., $a^{p-1} \equiv 1 \bmod p$.

[Remark: Mathematics is too big to be covered by a consistent notation. Sometimes we just have to jump from one notation to another and hope that we don't fall.]

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**.

(a): This part is just about sets and functions. For any subsets $S \subseteq G$ and $T \subseteq H$ we have

$$\begin{aligned}
S \subseteq \varphi^{-1}[T] &\Longleftrightarrow \text{"every element } s \in S \text{ satisfies } s \in \varphi^{-1}[T]\text{"} \\
&\Longleftrightarrow \text{"every element } s \in S \text{ satisfies } \varphi(s) \in T\text{"} \\
&\Longleftrightarrow \text{"if } h \in H \text{ has the form } h = \varphi(s) \text{ for some } s \in S \text{ then } h \in T\text{"} \\
&\Longleftrightarrow \text{"every element } h \in \varphi[S] \text{ satisfies } h \in T\text{"} \\
&\Longleftrightarrow \varphi[S] \subseteq T.
\end{aligned}$$

(b): Let $\varphi : (G, *, \varepsilon_G) \to (H, \bullet, \varepsilon_H)$ be a group homomorphism. Let $S \subseteq G$ be a subgroup and consider the image set $\varphi[S] \subseteq H$. For any two elements $a, b \in \varphi[S]$ we can write $a = \varphi(x)$ and $b = \varphi(y)$ for some $x, y \in S$. By properties of homomorphism we have

$$\varphi(x * y^{-1}) = \varphi(x) \bullet \varphi(y)^{-1} = a \bullet b^{-1}.$$

But since S is a subgroup we know that $x * y^{-1} \in S$ and hence $a \bullet b^{-1} \in \varphi[S]$. We have shown that $\varphi[S]$ is a subgroup of H.

(c): Let $\varphi : (G, *, \varepsilon_G) \to (H, \bullet, \varepsilon_H)$ be a group homomorphism. Let $T \subseteq H$ be a subgroup and consider the preimage set $\varphi^{-1}[T] \subseteq G$. For any two elements $a, b \in \varphi^{-1}[T]$ we have $\varphi(a) \in T$ and $\varphi(b) \in T$. Since T is a subgroup, this implies that

$$\varphi(a * b^{-1}) = \varphi(a) \bullet \varphi(b)^{-1} \in T,$$

and it follows that $a * b^{-1} \in \varphi^{-1}[T]$. We have shown that $\varphi^{-1}[T]$ is a subgroup of G.