ASSIGNMENT-1

1) Consider $H = \{1, a, b, c\}$. Consider an arbitrary $x, y \in H$. Is $xy = 1$? If so, it would be commutative. If suppose $xy \neq 1$. Is $xy = x$ or y? Neither, since that would result in either x or y being 1. Therefore, $xy = z$ where z is the element different from x, y. Same way, the argument can be extended to $yx = z$. Hence, either $xy = 1$, or $xy = yx = z$, which makes $\{1, a, b, c\}$ an abelian group.

Let us now classify the groups of order 4. We can immediately fill up the initial parts:

x	1	a	b	c
1	1	a	b	c
a	a	x	x	x
b	b	x	x	x
c	c	x	x	x

Since this is a finite group of order 4, there should be atleast one element with order 2. We WLOG select that element to be b so that $b^2 = 1$. Is $ab = a$ or b? Nope, since that would make either one identity. So $ab = c$. Is $ba = a$ or b? In much the same way, we conclude $ba = ab = c$. $b(ba) = bc = a$ and $(ab)b = ab^2 = cb$. Hence $bc = cb = a$. So far we got: (This is applicable for any group of size 4, since we did not use the property that this group has no element with order 4.)

x	1	a	b	c
1	1	a	b	c
a	a	x	c	x
b	b	c	1	a
c	c	x	a	x

(**The Klein Route**) Suppose our group has no element with order 4. Is $a^2 = b$? Can't be, because then, since $b^2 = 1$, we'd have $a^4 = 1$ which is against hypothesis. Hence $a^2 = 1$, or $a^2 = c$. Likewise, we can conclude that $c^2 = 1$ or $c^2 = a$ (Ask the same questions, is $c^2 = b$? No). Suppose $a^2 = 1$ and $c^2 = a$. That would make $c^4 = 1$, which is against hypothesis. Hence, if $a^2 = 1$ then $c^2 = 1$ as well. Likewise, if $c^2 = 1$, then $a^2 = 1$ as well. Suppose neither, i.e, $c^2 = a$ and $a^2 = c$. Then $c^4 = a^2 = c$ and $a^4 = c^2 = a$. We have $a^3 = 1$ and $c^3 = 1$. $(ba)a^2 = b$ which means $ca^2 = b \implies c^2 = b$. But $c^2 = a$. Absurd. Hence, this scenario is impossible. Hence, for the Klein route, $a^2 = c^2 = 1$.

Question for ac and ca, then arises. Is $ac = 1$? That would mean $a^2c = 1c = a$, absurd. Hence, $ac = b$. Similarly, is $ca = 1$? we would then have $c = a$ again. Therefore, $ac = ca = b$. This completes the Klein Route:

x	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

(**The $\mathbb{Z}/4\mathbb{Z}$ Route**) Suppose that G has an element of order 4. Since the size of the cyclic subgroup of this element is 4 as well, this group is cyclic. WLOG, assume that $G = \langle a \rangle$. Then every element is 1, $a = a$, $a^2 = b$, $a^3 = c$. We have (for a general 4 membered group)

x	1	a	b	c
1	1	a	b	c
a	a	x	c	x
b	b	c	1	a
c	c	x	a	x

Since the group is cyclic, we can immediately write $a^2 = b$. Since $a^3 = c$, $a^6 = a^2 = c^2 = b$. We can write that in as well. All that is left is ac and ca. Let us rule out the obvious: $ac \neq a$, $ca \neq a$, $ac \neq c$, $ca \neq q$. Is $ac = b$? That would mean $a^4 = b$, which makes $b = 1$. Same way, $ca \neq b$. Hence, ac and ca have only one option left, 1. We can fill that in to get the $\mathbb{Z}/4\mathbb{Z}$ isomorph:

x	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

Note that Klein is the unique 4 membered group with no element of order 4. $\mathbb{Z}/4\mathbb{Z}$ isomorph is the unique group with one element with order 4.

---

2) Suppose that $\forall x \in G$, $x^2 = 1$. Suppose there exists a, b so that $ab \neq ba$. This means $a^2 b \neq aba \implies b \neq aba$. This then means that $b^2 \neq (ba)(ba) = (ba)^2$. But this boils down to $1 \neq 1$. Absurd. Hence, $\forall a, b \in G$, $ab = ba$.

---

3) Suppose $a \in G$. Consider the case when order of a is finite$= n$. $a^n = 1$. $a \cdot a \cdot ... a = 1$. Note that $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$ which means that the inverse of a^n is $a^{-n} = (a^{-1})^n = 1$. $(a^{-1})^n = 1$ would mean that the actual order of a^{-1} is a divisor of n. Say order of a^{-1} is m. We have $m|n$. But the argument can be reversed with a^-1 as some b and a as some b^{-1} to get $n|m$ which gives $m = n$. Hence $\mathfrak{O}(a) = \mathfrak{O}(a^{-1})$.

---

4) Consider $\mathbb{Z}/6\mathbb{Z} \setminus \{0\}$. Let us define multiplication as $\overline{a} \times \overline{b} = \overline{(a \times b)}$. Consider the element $\overline{5}$. $3 \times 1 = 3mod(6)$. $3 \times 2 = 6mod6 = 0mod(6)$, $3 \times 3 = 3mod6$. $3 \times 4 = 12 = 0mod6$. $3 \times 5 = 15 = 3mod6$. Hence, we note that 3 has no inverse. Hence, $\mathbb{Z}_6$ is not a group.

Consider $\mathbb{Z}_7$. We know the classification of the elements in the multiplicative $(\mathbb{Z}_n)^*$, which is

$$(\mathbb{Z}_{n\mathbb{Z}})^* := \{z \in \mathbb{Z}/n\mathbb{Z} : \exists c \in \mathbb{Z}/n\mathbb{Z} : \overline{cz} = \overline{1}\}$$

Which is actually equivalent to saying

$$(\mathbb{Z}_{n\mathbb{Z}})^* := \{z \in \mathbb{Z}/n\mathbb{Z} : gcd(z, n) = 1\}$$

And we note that since 7 is a prime, every element smaller than 7 is coprimes with 7 which means that every element of $\mathbb{Z}/7\mathbb{Z} - \{0\}$ is in the multiplicative group.

---

5) $U_n :=$ the multiplicative $\mathbb{Z}_n$ which is $\{z \in \mathbb{Z}_n : \exists c \in \mathbb{Z}_n : cz = 1\}$, which can be rewritten as $\{z \in \mathbb{Z}_n : gcd(z, n) = 1\}$. Define $Aut(\mathbb{Z}_n, +)$ of the group $\mathbb{Z}_n$ as the set of all group isomorphisms from $\mathbb{Z}$ to itself, seen as a group under addition $+$.

Look at $aut(\mathbb{Z}_n, +)$, the set of all $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ such that it is a bijection (invertible) and is a homomorphism, i.e, $\forall x \in \mathbb{Z}_n$, we have $\phi(a + b) = \phi(a) + \phi(b)$. Let $\phi(a) = a'$. Define $\phi^{-1}(a') = a$. This is aswell a bijection. Consider $x, y \in \mathbb{Z}_n$ so that $\phi(a) = x$, $\phi(b) = y$. We know such unique a and b exist, since it is a bijection. Have a look at $\phi^{-1}(x)$ and $\phi^{-1}(y)$. We see that $\phi^{-1}(x) = a$ and $\phi^{-1}(y) = b$. What is $\phi^{-1}(x + y)$? $\phi^{-1}(\phi(a + b)) = a + b$. Hence, ϕ^{-1} is aswell a group isomorphism. Now consider $\phi \circ \phi^{-1}$ and $\phi^{-1} \circ \phi$ which is I the identity map. The identity map is an isomorphism. Therefore, for every element ϕ in Aut$(\mathbb{Z}_n, +)$, there exists an inverse ϕ^{-1}. Consider ϕ and ψ two group isomorphisms in aut. $\phi(a+b) = \phi(a)+\phi(b)$ and $\psi(a+b) = \psi(a)+\psi(b)$. Consider $\psi\circ\phi(a+b) = \psi(\phi(a)+\phi(b)) = \psi\circ\phi(a)+\psi\circ\phi(b)$. Hence, composition operation is also a group isomorphism (since bijectivity is preserved whenever we compose two bijections). Therefore, $Aut(\mathbb{Z}_n, +)$ is a group. This is true for any group as well.

Consider the map $\gamma : Aut(\mathbb{Z}_n, +) \to U_n$ given by $\gamma(\psi \in Aut(\mathbb{Z}_n, +)) = \psi(\overline{1})$ We have $\gamma(\psi) = \psi(\overline{1})$. $\gamma(\varphi) = \varphi(\overline{1})$. What is $\gamma(\psi \circ \varphi)$? it is $\psi \circ \varphi(\overline{1}) = \psi(\varphi(\overline{1}))$. What is $\gamma(\psi) \cdot \gamma(\varphi)$? It is $\psi(1) \cdot \varphi(1)$. Is $\psi(\varphi(1)) = \psi(1) \cdot \varphi(1)$?

We need to stop to understand that if ϕ is an automorphism from $\mathbb{Z}_n$ to itself, it must map 1 to an element $\overline{j} \in \mathbb{Z}_n$ so that $gcd(j, n) = 1$. To understand this, we note that $\mathbb{Z}_n$ is a cyclic group generated by 1. But we know that $\mathbb{Z}_n = \langle 1^x \rangle$ if and only if $gcd(x, n) = 1$. So j can generate $\mathbb{Z}_n$ if and only if $(j, n) = 1$. Moreover, if we are to preserve structure in the homomorphism ϕ, we need to map generators to generators. To see this, suppose $1 \mapsto k$ where $gcd(k, n) \neq 1$. Note that when we define a homomorphism on the generator, it is basically defined for every other element for $\phi(x) = \phi(1 + 1 + 1 \cdots 1) = x\phi(1)$. If $gcd(k, n) \neq 1$, then $\langle j \rangle$ will be a proper subgroup of $\mathbb{Z}_n$, meaning it will miss out on a few elements in $\mathbb{Z}_n$. Suppose $\phi(1) = j$, this means $\phi(x) = j^x = x(j)$ (in the context of an additive group). But All the multiples of j do not cover the entire group. Hence, ϕ, an automorphism, maps 1 to j so that $gcd(j, n) = 1$ or equivalently, ϕ maps 1 to an element in the multiplicative $(\mathbb{Z}_n)^*$ (since every element in the multiplicative group has its gcd with n to be 1). Notice that if

$a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n^*$, then $ab \in \mathbb{Z}_n^*$.

Now we can answer the question, is $\psi(\varphi(1)) = \psi(1)\varphi(1)$? $\psi(1) = k_1$ so that $(k_1, n) = 1$ and $\varphi(1) = j_1$ so that $(j_1, n) = 1$. $\psi(j_1) = j_1\psi(1)$ from the generator definition, hence we see that $\psi(\varphi(1)) = j_1 \times k_1 {=} \psi(1) \times \phi(1)$. Hence, this is a group homomorphism.

Now to show that γ is bijective, we note that, for a $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ to be an isomorphism, one needs to send a generator to a generator. i.e, different isomorphisms can be generated by sending 1 to each element j so that $(j, n) = 1$. Moreover, if we send 1 to a *non* generator, i.e an element with non unity gcd with n, then that ceases to be a group isomorphism since group order wouldn't be preserved. Hence, there are totient(n) elements in $Aut(\mathbb{Z}_n, +)$, which is the same as the size of the multiplicative group $\mathbb{Z}_n^*$. Hence, $\gamma : aut(\mathbb{Z}_n, +) \to U_n$ given by $\gamma(\psi) = \psi(1)$ is a group isomorphism.

---

6) Let $B_n := \{r \in \mathbb{Z}_n : gcd(r, n) = 1\}$ If $r, s \in B_n$ then $gcd(r, n) = gcd(s, n) = 1$. Consider $rs := \overline{rs} \in B_n$. $xr \equiv 1 mod(n)$ and $ys \equiv 1 mod(n)$. This means $xyrs \equiv 1 mod(n)$ which means $xyrs = 1 mod(n)$ which means $xyrs + zn = 1$. This means that $gcd(rs, n) = 1$.

Claim: Suppose $gcd(x, n) = 1$, and $x < n$ with $1 < n$, then for any z so that $z \in \overline{x}$, we have $gcd(z, n) = 1$.

Proof. Consider $z = rn + x$. We then have $n = px + q$ and we keep going to find the gcd as the final remainder in the process of euclid's division algorithm. Therefore, the *gcd* of z and n as well, is 1. □

Claim: Suppose $gcd(x, n) = j \neq 1(\geq 2)$ and $1 \leq x < n$ and $1 < n$. Then, the claim is that there exists $1 < b < n$ so that $xb \equiv 0 mod(n)$. This would then imply that there would exist no $z < n$ so that $xz \equiv 1 mod(n)$.

Proof. □