1. $\mathbb{Z}_5^\times$ is closed under multiplication since if $[a], [b] \in \mathbb{Z}_5^\times$, then $5 \nmid a, 5 \nmid b \Rightarrow 5 \nmid ab \Rightarrow [ab] \in \mathbb{Z}_5^\times$.

Identity. $[1]$ is identity:

$$[a]\cdot[1] = [a] = [1]\cdot[a] \qquad \forall [a] \in \mathbb{Z}_5^\times$$

Associativity. $([a]\cdot[b])\cdot[c] = [ab]\cdot[c] = [abc] = [a]\cdot[bc]$

$$= [a]([b]\cdot[c]).$$

Inverses. $\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$,

$[1]\cdot[1] = [1]$, (so $[1]^{-1} = [1]$)

$[2]\cdot[3] = [3][2] = [1]$, (so $[2]^{-1} = [3]$, $[3]^{-1} = [2]$)

$[4]\cdot[4] = [1]$ (so $[4]^{-1} = [4]$).

Cyclic? Yes, $[2]$ is a generator:

$[1] = [2]^0$, $[2] = [2]^1$, $[4] = [2]^2$, $[3] = [2]^3$.

Recall: If G is a finite cyclic group of order n, and if $d \mid n$, then $\exists!$ subgroup $H \subset G$ with $|H| = d$, and H is cyclic!

If $d \nmid n$, then $\neg\exists$ $H \subset G$ subgroup of order d.

(a) 49 has divisors $1, 7, 49 \Rightarrow$ 3 subgroups, all cyclic.

They are: $\langle 0 \rangle = \{0\}$, $\langle [7] \rangle$, $\langle [1] \rangle = \mathbb{Z}_{49}$.

(b) By the fact above, $\exists$ a subgroup of order 12 but not one of order 14, since $12 \mid 48$ but $14 \nmid 48$. The subgroup of order 12 is $\langle [4] \rangle$.

---

3. (a) Let $a, b \in G$. Then

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

(b) $$\#G = \#\{g \in G \mid g^2 = e\} + \#\{g \in G \mid g^2 \neq e\}$$
$$\#G = a, \quad \#\{g \in G \mid g^2 = e\} = b, \quad \#\{g \in G \mid g^2 \neq e\} = c$$

Claim. c is even.

Note. If we prove c is even, then we are done since a is even so $a = b + c \Rightarrow b$ is even. But $e \in \{g \in G \mid g^2 = e\}$, so b even $\Rightarrow \exists\, g \in G$ s.t. $g \neq e$ with $g^2 = e$.

Pf of Claim. Can write

$$C = \{g \in G \mid g^2 \neq e\} = \coprod_{g \in C} \{g, g^{-1}\},$$

and since $g \neq g^{-1}$ for $g \in C$, each $\#\{g, g^{-1}\} = 2$.

But this $\Rightarrow c$ is even.

---

4. (a) H is a subgroup: $e = g^0 \in H$. ✓

$g^k, g^\ell \in H \Rightarrow g^k \cdot g^\ell = g^{k+\ell} \in H$. ✓

$g^k \in H \Rightarrow (g^k)^{-2} = g^{-k} \in H$. ✓

H is cyclic since g is a generator: every element of H is a power of g.

(b) Let $H \subset G$ be a cyclic subgroup. Then $\exists\, g \in H$ s.t. g generates H, i.e., every $h \in H$ can be written $h = g^k$ for some $k \in \mathbb{Z}$. This $\Rightarrow H \subset \langle g \rangle$. But on the other hand, since H is closed under multiplication and inverses, and $g \in H$, all powers of g must be in $H \Rightarrow H = \langle g \rangle$.

---

5. $\{1\} = \langle 1 \rangle$, $\{1,-1\} = \langle -1 \rangle$, $\{1,-1,i,-i\} = \langle i \rangle = \langle -i \rangle$,

$\{1,-1,j,-j\} = \langle j \rangle = \langle -j \rangle$, $\{1,-1,k,-k\} = \langle k \rangle = \langle -k \rangle$.

---

6. (a) Identity: $(g,h)\cdot(e_G, e_H) = (ge_G, he_H) = (g,h)$

$(e_G, e_H)\cdot(g,h) = (e_G g, e_H h) = (g,h)$. ✓

Associativity. $((g_1,h_1)(g_2,h_2))(g_3,h_3) = (g_1g_2, h_1h_2)(g_3,h$

$= (g_1 g_2 g_3, h_1 h_2 h_3)$

$= (g_1,h_1)(g_2g_3, h_2h_3)$

$= (g_1,h_1)((g_2,h_2)(g_3,h_3))$ ✓

Inverses. Set $(g,h)^{-1} = (g^{-1}, h^{-1})$. Then

$(g,h)(g,h)^{-1} = (gg^{-1}, hh^{-1}) = (e,e)$

$(g,h)^{-1}(g,h) = (g^{-1}g, h^{-1}h) = (e,e)$ ✓

(b) (1,1) is a generator: We can either show this directly, or, note that if

$n \cdot (1,1) = (n,n) = (0,0)$, then

$2 \mid n$ and $5 \mid n \implies 10 \mid n$, so $(1,1)$ has order $10 = |\mathbb{Z}_2 \times \mathbb{Z}_5|$.

If $\mathbb{Z}_3 \times \mathbb{Z}_3$ were cyclic, it would have an element of order 9, but all elements have order dividing 3 since $3([a],[b]) = ([3a],[3b])$

$= ([0],[0])$.

So not cyclic.

By Lagrange's theorem, $\mathbb{Z}_5 \times \mathbb{Z}_5$ can have subgroups of order 1, 5, 25. Of these, the subgroup of order 25 (i.e. $\mathbb{Z}_5 \times \mathbb{Z}_5$ itself) is not cyclic, since every element is killed by 5. The subgroup of order 1, i.e., $\{0\}$, is cyclic, and since 5 is prime, so are all subgroups of order 5! Furthermore, every nonzero element of a cyclic group of order 5 is a generator, also since 5 is prime. That is, each subgroup of order 5 has 4 generators. Since each of the 24 elements of $G \setminus \{e\}$ has order 5, each such element generates a subgroup of order 5, but each subgroup has 4 generators $\implies \frac{24}{4} = 6$ subgroups of order 5 + (1) of order 1 $\implies$ (7) cyclic subgroups.