HW3 SOLUTION

JI ZENG

Only problems with provided solutions will be graded. Solutions might be concise for some problems, but please be noticed that they don't reflect the wanted level of detailedness of your answer.

Armstrong.4.6
By hypothesis we have $x^2 = y^2 = (xy)^2 = e$. So

$$\begin{aligned} & xy = yx \\ \iff & yxy = yyx \\ \iff & yxy = x, \text{b/c } yy = e \\ \iff & xyxy = xx \\ \iff & (xy)^2 = e, \text{b/c } xx = e. \end{aligned}$$

Since the last identity is given true, we conclude the proof.

Armstrong.4.8
Notice that we have $(gxg^{-1})^n = \underbrace{gxg^{-1}gxg^{-1}\dots gxg^{-1}}_{n-times} = gx^ng^{-1}$. Then

$$x^n = e \iff gx^ng^{-1} = e \iff (gxg^{-1})^n = e.$$

Hence we have two sets equal

$$\{n \in \mathbb{N} | x^n = e\} = \{n \in \mathbb{N} | (gxg^{-1})^n = e\}.$$

Then clearly $\text{ord}(x) := \min\{n \in \mathbb{N} | x^n = e\} = \min\{n \in \mathbb{N} | (gxg^{-1})^n = e\} =: \text{ord}(gxg^{-1})$.

Problem.B
(a) Notice that $gcd(5, 12) = 1$ (Or you can just say "take $a = 5$"), so $\exists a$ s.t. $a5 \equiv 1 \pmod{12}$.
Then $\forall [m] \in \mathbb{Z}_{12}$, take $k = ma$ we have

$$k5 \equiv ma5 \equiv m \pmod{12}.$$

Then means $k[5] = [m] \in \mathbb{Z}_12$, hence $[m] \in \langle [5] \rangle, \forall [m]$ as wanted.
(b) By the argument in (a), every $[n]$ s.t. n and 12 are coprime is a generator. Conversely, if $[n]$ is a generator, then $\exists k \in \mathbb{N}$ s.t. $k[n] = [1] \in \mathbb{Z}_{12}$, which means

$$kn \equiv 1 \pmod{12}$$

but this implies $gcd(n, 12) = 1$. Therefore, $[n]$ is a generator **iff** n and 12 are coprime. Hence they're $[1], [5], [7], [11]$.
(You should check the "**iff**" to claim you have found "all" generators.)

(c) $\langle[3]\rangle = \{[3],[6],[9],[12]=[0]\}$ and $\langle[4]\rangle = \{[4],[8],[12]=[0]\}$.

Problem.C

(a) Just check $\langle[2]\rangle = \{[2],[4],[8],[16]=[3],[6],[12],[24]=[11],[22]=[9],[18]=[5],[10],[20]=[7],[14]=[1]\}$. Notice $\langle[2]\rangle = \mathbb{Z}_{13}^*$, so $\mathbb{Z}_{13}^*$ is cyclic with generator [2].
(b) Since $\mathbb{Z}_{13}^*$ is cyclic with generator [2] and $|\mathbb{Z}_{13}^*| = 12$. We have an **isomorphism**

$$f : (\mathbb{Z}_{12}, +) \to (\mathbb{Z}_{13}^*, *), \quad [1]_{12} \mapsto [2]_{13}.$$

Then by the principle of isomorphism we are led to find the generators of $\mathbb{Z}_{12}$, which are $[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}$.
Hence the generators of $\mathbb{Z}_{13}^*$ are $f([1]_{12}) = [2]_{13}, f([5]_{12}) = [2^5]_{13} = [6]_{13}, f([7]_{12}) = [2^7]_{13} = [11]_{13}, f([11]_{12}) = [2^1 1]_{13} = [7]_{13}$.
(c) $\langle[3]\rangle = \{[3],[9],[27]=[1]\}$ and $\langle[4]\rangle = \{[4],[16]=[3],[12],[48]=[9],[36]=[10],[40]=[1]\}$.

Problem.D

(a) Check the following things to claim $G \times H$ is a group.
$\bullet$ is indeed a composition law (i.e. $G \times H$ is closed under multiplication): Leave to reader.
$\bullet$ is associative: Leave to reader.
Existence of identity: Write 1_G and 1_H the identities of G and H resp. (respectively). Consider $1_{G\times H} := (1_G, 1_H) \in G \times H$. For any (g,h)

$$1_{G\times H} \bullet (g,h) = (1_G * g, 1_H \star h) = (g,h),$$

and similarly $(g,h) \bullet 1_{G\times H} = (g,h)$. So $1_{G\times H}$ is the identity.
Existence of inverse: For any $(g,h) \in G \times H$

$$(g^{-1}, h^{-1}) \bullet (g,h) = (g^{-1} * g, h^{-1} \star h) = (1_G, 1_H) = 1_{G\times H},$$

and similarly $(g,h) \bullet (g^{-1}, h^{-1}) = 1_{G\times H}$. Hence $G \times H \ni (g^{-1}, h^{-1}) = (g,h)^{-1}$ is the inverse.
(b) Write $LHS := \mathrm{ord}(g,h)$ and $RHS := lcm(\mathrm{ord}(g), \mathrm{ord}(h))$.
We first prove $LHS \leq RHS$. Notice $\mathrm{ord}(g)|RHS$ and $\mathrm{ord}(h)|RHS$ by the definition of least common multiple, so $g^{RHS} = 1_G$ and $h^{RHS} = 1_H$. Hence $(g,h)^{RHS} = (1_G, 1_H) = 1_{G\times H}$. So $RHS \in \{n|(g,h)^n = 1_{G\times H}\}$. We also know $LHS = \min\{n|(g,h)^n = 1_{G\times H}\}$ by definition of order, so $LHS \leq RHS$.
Now we prove $LHS \geq RHS$. Again by definition of order, $(g,h)^{LHS} = 1_{G\times H}$, which means $g^{LHS} = 1_G$ and $h^{LHS} = 1_H$. By property of order, we have $\mathrm{ord}(g)|LHS$ and $\mathrm{ord}(h)|LHS$, i.e. LHS is a common multiple of $\mathrm{ord}(g)$ and $\mathrm{ord}(h)$. So by definition of least common multiple (a.k.a. lcm), $LHS \geq RHS$.
Therefore we conclude $LHS = RHS$.
(c) By hypothesis, we have a generator $g \in G$ s.t. $\mathrm{ord}(g) = |G|$ and similarly a generator $h \in H$ s.t. $\mathrm{ord}(h) = |H|$. By (b)

$$\begin{aligned}(ord)(g,h) &= lcm(\mathrm{ord}(g), \mathrm{ord}(h)) \\ &= lcm(|G|, |H|) = |G||H|, \text{ b/c } gcd(|G|,|H|) = 1 \\ &= |G \times H|,\end{aligned}$$

which means (g,h) is a generator for $G \times H$.
(d) Write $|G| = m$ and $|H| = n$, by hypothesis we have $gcd(m,n) = 1$. Hence by

Chinese Remainder Theorem, we have an isomorphism

$$\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad [x]_{mn} \mapsto ([x]_m, [x]_n).$$

Hence $\mathbb{Z}_{mn}$ being cyclic implies $\mathbb{Z}_m \times \mathbb{Z}_n$ being cyclic.
Let $g \in G$ and $h \in H$ be generators resp. then we have isomophisms

$$f_1 : \mathbb{Z}_m \to G, \quad [1]_m \mapsto g;$$
$$f_2 : \mathbb{Z}_n \to H, \quad [1]_n \mapsto h.$$

Hence we have an isomorphism

$$F : \mathbb{Z}_m \times \mathbb{Z}_n \to G \times H, \quad ([a]_m, [b]_n) \mapsto (f_1([a]_m), f_2([b]_n)).$$

Therefore, as $\mathbb{Z}_m \times \mathbb{Z}_n$ and $G \times H$ are isomorphic, the former one being cyclic implies the latter one being cyclic, as wanted.