$= [a^{-mn}]^{-1}$

$= a^{mn}$, by (i) of Theorem 6.

Thus, $\forall\ m, n \in \mathbb{Z}$, (iii) holds.

E19) i) Since $b \in G$, $b^m \in G$. So $ab^m = b^m a$, as G is abelian.

ii) If $m = 0$, $(ab)^m = e$, $a^m = e$, $b^m = e$. Hence, $(ab)^m = a^m b^m$.

If $m > 0$, use induction on m to prove it.

If $m < 0$, then $(ab)^{-m} = a^{-m} \cdot b^{-m}$, since $(-m) > 0$.

$\Rightarrow a^m (ab)^{-m} = b^{-m}$

$\Rightarrow a^m = b^{-m}(ab)^m$

$\Rightarrow b^m a^m = (ab)^m$

$\Rightarrow a^m b^m = (ab)^m$, since G is abelian.

E20) Note that $+$ is a binary operation over $\mathbb{Z}_5$.

Hence, the table must have entries from $\mathbb{Z}_5$ only. Thus, it is as below:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Did you notice that the entries are symmetric about the diagonal from $\bar{0} + \bar{0}$ to $\bar{4} + \bar{4}$? What does this tell you about the operation?

E21) From the discussion before the exercises, you know that $\cdot$ is an abelian associative binary operation on $\mathbb{Z}_5^*$, with identity $\bar{1}$. Thus, the table is as below:

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

The Cayley table above shows that for each $\bar{r} \in \mathbb{Z}_5^*$, $\exists\ \bar{s} \in \mathbb{Z}_5^*$ s.t. $\bar{r} \cdot \bar{s} = \bar{1}$. Hence, $(\mathbb{Z}_5^*, \cdot)$ is an abelian group.

E22) i) You can form the Cayley table of multiplication over $\mathbb{Z}_{11}^*$ and obtain the inverses as follows.

$\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{6}$, $\bar{6}^{-1} = \bar{2}$, $\bar{3}^{-1} = \bar{4}$, $\bar{4}^{-1} = \bar{3}$, $\bar{5}^{-1} = \bar{9}$, $\bar{9}^{-1} = \bar{5}$, $\bar{7}^{-1} = \bar{8}$, $\bar{8}^{-1} = \bar{7}$, $\overline{10}^{-1} = \overline{10}$.

ii) For $\bar{r} \in \mathbb{Z}_p^*$, $(r, p) = 1 \Rightarrow rs + pt = 1$ for some $s, t \in \mathbb{Z}$.

$\Rightarrow \bar{r}\,\bar{s} \equiv \bar{1} (\mathrm{mod}\, p) \Rightarrow \bar{r}^{-1} = \bar{s}$.

Since $s \in \mathbb{Z} = \bigcup_{i=0}^{p-1} \bar{i}$, $\exists\ \bar{m} \in \mathbb{Z}_p$ s.t. $\bar{s} = \bar{m}$, $0 \le m \le (p-1)$.

However, since $\bar{r}\bar{s} = \bar{1}$, $\bar{s} \neq \bar{0}$ in $\mathbb{Z}_p$. Hence, $\bar{m} \neq \bar{0}$, i.e., $0 < m \le (p-1)$.

For example, $\bar{1}^{-1} = \bar{1}$ since $1 \cdot 1 + p \cdot 0 = 1$. (Here $t = 0$.)

Again $(\overline{p-1})^{-1} = \overline{p-1}$, since $(p-1)^2 \equiv 1 (\mathrm{mod}\, p)$. (Note that $(p-1)(p-1) + p(2-p) = 1$.)

iii) **Multiplication is closed on $\mathbb{Z}_p^*$:** For $\bar{r}, \bar{s} \in \mathbb{Z}_p^*$, $p \not| r$ and $p \not| s$.

Since p is a prime, $p \not| rs$. Thus, $\overline{rs} = \bar{r}\bar{s} \in \mathbb{Z}_p^*$.

Multiplication is associative and commutative over $\mathbb{Z}_p^*$, since it is so over $\mathbb{Z}_p$.

$\bar{1}$ is the multiplicative identity, as discussed earlier.

Every element has an inverse w.r.t. multiplication, as shown in (ii) above.

Thus, $(\mathbb{Z}_p^*, \cdot)$ is an abelian group.

E23) $f = (1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$.

So $f^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = f$.

Thus, f^{-1} is a cycle also.

E24) $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

The Cayley table is

$\circ$	I	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
I	I	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	I	$(1\ 3\ 2)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	I	$(1\ 3\ 2)$	$(1\ 2)$	$(2\ 3)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	I	$(1\ 3)$	$(1\ 2)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3\ 2)$	I
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	I	$(1\ 2\ 3)$

From the table, we see that $I^{-1} = I$, $(1\ 2)^{-1} = (1\ 2)$, $(1\ 3)^{-1} = (1\ 3)$, $(2\ 3)^{-1} = (2\ 3)$, $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$, $(1\ 3\ 2)^{-1} = (1\ 2\ 3)$.

E25) Check that $(1\ 2)^{-1} = (1\ 2)$ and $(2\ 4\ 5)^{-1} = (2\ 5\ 4)$.

Now $(1\ 2) \circ (2\ 4\ 5) = (2\ 4\ 5\ 1)$.

You should check that $[(1\ 2) \circ (2\ 4\ 5)]^{-1} = (1\ 5\ 4\ 2)$.

Also $(1\ 2)^{-1} \circ (2\ 4\ 5)^{-1} = (1\ 2) \circ (2\ 5\ 4) = (2\ 5\ 4\ 1) \neq (1\ 5\ 4\ 2)$, since, for example, $(2\ 5\ 4\ 1)$ maps 2 to 5 and $(1\ 5\ 4\ 2)$ maps 2 to 1.

E26) Consider $(1\ 2\ 3) \in S_4$. This does not lie in D_8 since if you move the vertices $1, 2$ and 3 of the square, then you have to move vertex 4 also. But $(1\ 2\ 3)$ leaves 4 fixed and moves the other 3 elements.

E27) $D_{10} = \{I, r, R, R^2, R^3, R^4, rR, rR^2, rR^3, rR^4\}$, where $r^2 = I$, $R^5 = I$ and $rR = R^4r$.

$\circ$	I	r	R	R^2	R^3	R^4	rR	rR^2	rR^3	rR^4
I	I	r	R	R^2	R^3	R^4	rR	rR^2	rR^3	rR^4
r	r	I	rR	rR^2	rR^3	rR^4	R	R^2	R^3	R^4
R	R	rR^4	R^2	R^3	R^4	I	r	rR	rR^2	rR^3
R^2	R^2	rR^3	R^3	R^4	I	R	rR^4	r	rR	rR^2
R^3	R^3	rR^2	R^4	I	R	R^2	rR^3	rR^4	r	rR
R^4	R^4	rR	I	R	R^2	R^3	rR^2	rR^3	rR^4	r
rR	rR	R^4	rR^2	rR^3	rR^4	r	I	R	R^2	R^3
rR^2	rR^2	R^3	rR^3	rR^4	r	rR	R^4	I	R	R^2
rR^3	rR^3	R^2	rR^4	r	rR	rR^2	R^3	R^4	I	R
rR^4	rR^4	R	r	rR	rR^2	rR^3	R^2	R^3	R^4	I

E28) No. For example, from the operation table in Example 13, you can see that $r_1 \circ R_{90} \neq R_{90} \circ r_1$ in D_8, since $r_4 \neq r_3$.
In general, $rR = R^{n-1}r \neq Rr$ unless $n = 2$.

E29) Since $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$.
Similarly, check that $B^2 = A^2$, $B^4 = I$ and $BA = -AB = A^3B$, since $-A = (-I)A = A^2 \cdot A = A^3$.
Thus, the table for $(Q_8, \cdot)$ is as below:

$\cdot$	I	A	A^2	A^3	B	AB	A^2B	A^3B
I	I	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	I	AB	A^2B	A^3B	B
A^2	A^2	A^3	I	A	A^2B	A^3B	B	AB
A^3	A^3	I	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	A^2	A	I	A^3
AB	AB	B	A^3B	A^2B	A^3	A^2	A	I
A^2B	A^2B	AB	B	A^3B	I	A^3	A^2	A
A^3B	A^3B	A^2B	AB	B	A	I	A^3	A^2

Since $BA \neq AB$, Q_8 is not abelian.
Also, Q_8 has 8 elements. Hence, $o(Q_8) = 8$.

E30) Elementwise multiplication is a well-defined operation on $\mathbb{M}_{m\times n}(\mathbb{C})^*$.
However, it is not closed on $\mathbb{M}_{m\times n}(\mathbb{C})^*$, because, for example,
$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in \mathbb{M}_2(\mathbb{C})^*$, but

$$A \cdot B = \begin{bmatrix} 1\cdot 0 & 0\cdot 1 \\ 0\cdot 0 & 0\cdot 0 \end{bmatrix} = \mathbf{0} \notin \mathbb{M}_2(\mathbb{C})^*.$$

Hence, $(\mathbb{M}_{m\times n}(\mathbb{C})^*, \cdot)$ is not a group.

E31) Note that $0 = 1-\zeta^n = (1-\zeta)(1+\zeta+\zeta^2+\cdots+\zeta^{n-1})$ in $\mathbb{C}$.

Also $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \neq 1$ since $n > 1$.

Hence, $1+\zeta+\zeta^2+\cdots+\zeta^{n-1} = 0$.

E32) The cube roots of unity are 1, $\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$, $\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$,

i.e., 1, ω, ω^2, where $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1}{2} + i\frac{\sqrt{3}}{2} = \frac{-1+i\sqrt{3}}{2}$.

By E31, $1+\omega+\omega^2 = 0$. $\therefore \omega^2 = -(1+\omega) = \frac{-1-i\sqrt{3}}{2}$.

E33) $U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$, where $\zeta = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$.

So the table for $(U_6, \cdot)$ is as below:

$\cdot$	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
1	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
ζ	ζ	ζ^2	ζ^3	ζ^4	ζ^5	1
ζ^2	ζ^2	ζ^3	ζ^4	ζ^5	1	ζ
ζ^3	ζ^3	ζ^4	ζ^5	1	ζ	ζ^2
ζ^4	ζ^4	ζ^5	1	ζ	ζ^2	ζ^3
ζ^5	ζ^5	1	ζ	ζ^2	ζ^3	ζ^4

Now, you know that $D_6 = S_3$. In E24 you have given the Cayley table of this group. If you compare the tables, you can see that the one above corresponds to a commutative operation, while the one in E24 does not.

Hence, $(U_6, \cdot)$ and $(D_6, \circ)$ are different in structure.

E34) $*$ **is associative:** Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$.

Use the fact that $*_1$ and $*_2$ are associative to prove that $((a_1, b_1)*(a_2, b_2))*(a_3, b_3) = (a_1, b_1)*((a_2, b_2)*(a_3, b_3))$, i.e., $*$ is associative.

The identity element w.r.t. $*$: The identity w.r.t. $*$ is (e_1, e_2), where e_1 and e_2 are the identities in G_1 and G_2, respectively. This is because $(a, b)*(e_1, e_2) = (a *_1 e_1, b *_2 e_2) = (a, b)\ \forall\ (a, b) \in G$.

The inverse w.r.t. $*$: You should check that the inverse of $(x, y) \in G$ is (x^{-1}, y^{-1}), where $x *_1 x^{-1} = e_1$, $y *_2 y^{-1} = e_2$.

E35) First let us assume $G_1 \times G_2$ is abelian.

Now, for any $a, c \in G_1$, $b, d \in G_2$,

$(a, b)(c, d) = (c, d)(a, b)$, i.e., $(ac, bd) = (ca, db)$.

Thus, $ac = ca$ and $bd = db$.
Hence, G_1 and G_2 are abelian.

You should prove the converse. For this, you can move in the reverse direction along the path of the argument above.

E36) Consider $(\{0\}, +)$ and $(\mathbb{Z}, +)$. Then $\{0\} \times \mathbb{Z} = \{(0, m) | m \in \mathbb{Z}\}$ is infinite, but $\{0\}$ is finite. Hence, $G_1 \times G_2$ being infinite does not require both G_1 and G_2 to be infinite.
If either of G_1 or G_2 is infinite, then $G_1 \times G_2$ is infinite.
Hence, $G_1 \times G_2$ being finite requires both to be finite.

E37) $U_3 \times S_3 = \{(x, y) | x \in U_3, y \in S_3\}$.
Now $U_3 = \{1, \omega, \omega^2\}$ (see E32).
Also S_3 is as in E24.
So $|U_3 \times S_3| = 3 \times 6 = 18$, i.e., $o(U_3 \times S_3) = 18$.
We will start you off on the table. You should complete it.

$\bullet$	$(1, I)$	$(\omega, (1\ 2))$	…
$(1, I)$	$(1, I)$	$(\omega, (1\ 2))$	…
$(\omega, (1\ 2))$	$(\omega, (1\ 2))$	(ω^2, I)	…
⋮	⋮	⋮	…