**4.4.** Theorem 4.4(iii) gives a formula

$$o(x^m) = \frac{o(x)}{\gcd(m, o(x))}$$

for $x$ in a group (written using multiplicative notation). The order of 1 in $\mathbb{Z}_{30}$ is 30. Thus, the order of $m = m \cdot 1$ in $\mathbb{Z}_{30}$ is $30/\gcd(30, m)$. We obtain $o(3) = 10$, $o(4) = 15$, $o(6) = 5$, $o(7) = 30$, and $o(18) = 5$.

**4.5.**

Using the formula from the previous problem, we have $o(x^m) = 18/\gcd(18, m)$. Thus, $o(x^2) = 9$, $o(x^3) = 6$, $o(x^4) = 9$, $o(x^5) = 18$, and $o(x^{12}) = 3$.

**4.10.**

**(a)** To check that the binary operation is well-defined, we need to check that $a \odot b = \overline{ab} \neq 0$ for all $a, b \in \{1, \ldots, 6\}$. This occurs only when $ab$ is divisible by 7. Since 7 is prime and each of $1, 2, 3, 4, 5, 6$ are not divisible by 7, $ab$ is never divisible by 7. Thus, the operation is well-defined.

To prove associativity, we need to verify that $\overline{\overline{ab}c} = \overline{a\overline{bc}}$ for all $a, b, c \in G$. Note that $ab = 7k + \overline{ab}$ for some $k \in \mathbb{Z}$. Thus $abc = (7k + \overline{ab})c = 7kc + \overline{ab}c$. Therefore $abc \equiv \overline{ab}c \mod 7$. Thus $\overline{abc} = \overline{\overline{ab}c}$. Similarly, $\overline{a\overline{bc}} = \overline{abc}$.

The identity is 1 and we find all inverses explicitly:

$$1^{-1} = 1,\ 2^{-1} = 4,\ 3^{-1} = 5,\ 4^{-1} = 2,\ 5^{-1} = 3,\ 6^{-1} = 6.$$

**(b)** The group is cyclic with generator 3:

$$\{\ldots, \overline{3^0}, \overline{3^1}, \overline{3^2}, \overline{3^3}, \overline{3^4}, \overline{3^5}, \ldots\} = \{1, 3, 2, 6, 4, 5\}.$$

**4.13.**

Let $x$ be an element of $G$. Since $G$ is finite, we know that the set $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ is finite. Thus, by the Pigeonhole Principle, there exist some $j, k \in \mathbb{Z}$ such that $x^j = x^k$. Thus $x^{j-k} = e$. We conclude that $x$ has finite order.

**4.17.**

Suppose $y$ is another generator of $G$. Since $G = \langle x \rangle$, this means that $y = x^m$ for some $m \in \mathbb{Z}$. Since $G = \langle y \rangle$, this means that $x = y^k$ for some $k \in \mathbb{Z}$. Thus $y = x^m = (y^k)^m = y^{km}$. Thus $km = 1$. The only integer values for $k, m$ are $-1$ and 1 as desired.

**4.20.**

Let $b$ be a conjugate of $a$. Then $b = xax^{-1}$. Suppose $a$ has finite order $n$. Observe that

$$\begin{aligned} b^n &= \left(xax^{-1}\right)^n \\ &= \underbrace{\left(xax^{-1}\right)\left(xax^{-1}\right)\cdots\left(xax^{-1}\right)}_{n \text{ times}} \\ &= xa(x^{-1}x)a(x^{-1}x)a\cdots a(x^{-1}x)ax^{-1} \\ &= xa(e)a(e)a\cdots a(e)ax^{-1} \\ &= x\underbrace{(a\cdots a)}_{n \text{ times}}x^{-1} \\ &= xa^nx^{-1} = xx^{-1} = e\ . \end{aligned}$$

Thus, $b$ has finite order less than or equal to $n$.

We have shown that if $b$ is a conjugate of $a$ and $a$ has finite order $n$, then $o(b) \leq o(a)$. Observe that $a = x^{-1}bx$, so $a$ is a conjugate of $b$. Thus $o(a) \leq o(b)$ if $b$ has finite order. Thus, they are either both of infinite order or they both have finite order and $o(a) = o(b)$.

**4.21.**

Suppose $xy$ has finite order $n$. This means that $e = (xy)^n$. Multiplying on the left by $y$ and the right by $y^{-1}$ we obtain $yey^{-1} = y(xy)^ny^{-1}$. Thus

$$\begin{aligned} e &= y\underbrace{(xy)\,(xy)\cdots(xy)\,(xy)}_{n \text{ times}}y^{-1} \\ &= y\underbrace{(xy)\,(xy)\cdots(xy)}_{n-1 \text{ times}}x \\ &= \underbrace{(yx)\,(yx)\cdots(yx)}_{n-1 \text{ times}}yx \\ &= (yx)^n \end{aligned}$$

We conclude that, if $xy$ has finite order, then $o(yx) \leq o(xy)$. Replacing the roles of $x$ and $y$, if $yx$ has finite order, then $o(xy) \leq o(yx)$. Thus, they are either both of infinite order or they both have finite order and $o(xy) = o(yx)$.