Exercise 1 (page 69)

For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the orders of the group?

	Z_{12}	U(10)	U(12)	U(20)	D_4
Group Order:	12	4	4	8	8

Element Orders:

Z_{12}: 0, 12, 6, 4, 3, 12, 2, 12, 6, 12, 6, 12
U(10): |1|: ∞ , |3|: 10, |7|: 10, |9|: 10
U(12): |1|: ∞ , |5|: 12, |7|: 12, |11|: 12
U(20): |1|: ∞ , |3|: 20, |7|: 20, |9|: 20, |11|: 20, |13|: 20, |17|: 20, |19|: 20
D_4: 0, 4, 2, 4, 2, 0, 2, 0

It looks like the orders of the elements of the group can never be bigger than the order of the group itself.

Exercise 2

Let Q be the group of rational numbers under addition and let $\mathbf{Q}^*$ be the group of nonzero rational numbers under multiplication.
In Q, list the elements in in $\langle\frac{1}{2}\rangle$.
$\langle\frac{1}{2}\rangle = \{ \frac{n}{2} \ \mid \text{n} \in \mathbb{Z} \ \} = \{ ... \ \frac{-3}{2}, \frac{-2}{2}, \frac{-1}{2}, \frac{-0}{2}, \frac{1}{2}, \frac{2}{2}, \frac{3}{2}, ... \}$
In $\mathbf{Q}^*$, list the elements in $\langle\frac{1}{2}\rangle$.
$\langle\frac{1}{2}\rangle = \{ (\frac{1}{2})^n \ \mid \text{n} \in \mathbb{Z} \ \} = \{ ... \ (\frac{1}{2})^{-3}, (\frac{1}{2})^{-2}, (\frac{1}{2})^{-1}, (\frac{1}{2})^{0}, (\frac{1}{2})^{1}, (\frac{1}{2})^{2}, (\frac{1}{2})^{3}, ... \}$

Exercise 4

Prove that in any group, an element and its inverse have the same order.

Proof.

Let g $\in$ G. By definition, $\text{g}^{-1} \in$ G exists.
Let n = |g| and m = $|\text{g}^{-1}|$
Want to show: n = m
Suppose not. Suppose that either n > m or m > n.
By definition,
g^n = e
$(\text{g}^{-1})^m$ = e
So,
$\text{g}^n * (\text{g}^{-1})^m$ = e * e = e
g * g * g ... (n times) * $\text{g}^{-1} * \text{g}^{-1} * \text{g}^{-1}$ ... (m times) = e
Without loss of generality, let's assume m is bigger.
Then $\text{g}^{-1} * \text{g}^{-1}$ ... (m − n times) = e.
However, since n is a positive integer, m − n < m
(a contradiction, since m is the smallest possible positive integer such that $(\text{g}^{-1})^m$ = e)

□

Exercise 13

For any group elements a, x $\in$ G, prove that $|\mathbf{xax}^{-1}| = |\mathbf{a}|$. This exercise is referred to in Chapter 13.

Proof.

Let m be the order of xax^{-1}, and n be the order of a.
Want to show: m = n
By definition,
(xax^{-1})^{m} = e
(xax^{-1}) * (xax^{-1}) * ... (xax^{-1}) (m times) = e
xa^{m}x^{-1} = e
x^{-1} xa^{m}x^{-1} = x^{-1} e
a^{m}x^{-1} = x^{-1}
a^{m}x^{-1}x = x^{-1}x
a^{m} = e
Since both a^{m} = e and a^{n} = e, and both are defined to be the minimum positive integer that makes the equation true, they both have to be the same minimum positive integer.

□