7.4.10 If \( f : G \to H \) is a surjective homomorphism of groups and \( G \) is abelian, prove that \( H \) is abelian.

Suppose \( a, b \in H \). Then there are \( a', b' \in G \) such that \( f(a') = a \) and \( f(b') = b \) (because \( f \) is surjective). Thus \( ab = f(a')f(b') = f(a'b') = f(b'a') = f(b')f(a') = ba \) and hence \( H \) is abelian (we used both that \( f \) is a homomorphism and that \( G \) is abelian).

7.4.16 Let \( G \) be a multiplicative group and \( c \) a fixed element of \( G \). Let \( H \) be the set \( G \) equipped with a new operation \( * \) defined by \( a * b = abc \).

(a) Prove that \( H \) is a group.

In order to prove that \( H \) is a group under \( * \), we need to check the four group axioms.

\*-Closure: It is clear that \( H \) is closed under \( * \) because \( a * b = abc \) is still an element of the set \( G \).

\*-Associativity: Let \( a, b, d \in H \). Then \( (a * b) * d = (abc) * d = acbcd = ac(b * d) = a * (b * d) \), so associativity holds (note that we used that the product in \( G \) is associative).

\*-Identity: We claim that \( c^{-1} \) is the identity in \( H \). Indeed, if \( a \in H \), then \( a * c^{-1} = acc^{-1} = ae = a \) and \( c^{-1} * a = c^{-1}ca = ea = a \) as required.

\*-Inverses: Let \( a \in H \) and consider the element \( c^{-1}a^{-1}c^{-1} \). Here \( a * (c^{-1}a^{-1}c^{-1}) = acc^{-1}a^{-1}c^{-1} = aea^{-1}c^{-1} = a^{-1}c^{-1} = c^{-1} = c^{-1} \) and \( (c^{-1}a^{-1}c^{-1}) * a = c^{-1}a^{-1}c^{-1}ca = c^{-1}a^{-1}a = c^{-1} \), so that \( c^{-1}a^{-1}c^{-1} \) is the *-inverse of \( a \in H \) (because \( c^{-1} \) is the identity), and thus *-inverses exist.

(b) Prove that the map \( f : G \to H \) given by \( f(x) = c^{-1}x \) is an isomorphism.

The map \( f \) is clearly surjective because if \( a \in H \), then \( ca \in G \), and \( f(ca) = c^{-1}ca = a \). Injectivity is similarly clear. If \( f(a) = f(b) \) for some \( a, b \in G \), then \( c^{-1}a = c^{-1}b \) as elements of \( H \), and thus \( c^{-1}a = c^{-1}b \) as elements of \( G \) as well (the elements of \( G \) and \( G \) are given by the same set,
after all). In \( G \) we can cancel the \( c^{-1} \) from each side of this equation, and get that \( a = b \) as required.

So it remains to show that \( f \) is a homomorphism. Let \( a, b \in G \). Then
\[
\begin{align*}
f(ab) &= c^{-1}(ab) = c^{-1}aeb = c^{-1}a(cc^{-1})b = (c^{-1}a)(c^{-1}b) = (c^{-1}a) \ast (c^{-1}b) = f(a)f(b),
\end{align*}
\]
so \( f \) is a homomorphism. Because \( f \) is also a bijection, we conclude that it is an isomorphism.

**7.5.4** Suppose \( G \) is the cyclic group \( \langle a \rangle \) and \( |a| = 15 \). If \( K = \langle a^3 \rangle \), list all the distinct cosets of \( K \) in \( G \).

We know by theorem 7.8 that \( |a^3| = 5 \). So by Lagrange’s theorem there are 3 distinct cosets of \( K \) in \( G \). They are \( K = \langle e, a^3, a^9, a^{12} \rangle \), \( Ka = \langle a, a^4, a^7, a^{10}, a^{13} \rangle \), and \( Ka^2 = \langle a^2, a^5, a^8, a^{11}, a^{14} \rangle \). (\( K \) is the obvious first choice, then we can find the other cosets by considering \( Ka^i \) for some \( i \) such that \( a^i \) is not in any of our previous choices).

**7.5.8** A group \( G \) has fewer than 100 elements and subgroups of orders 10 and 25. What is the order of \( G \)?

We know by Lagrange’s theorem that 10 and 25 both divide \( |G| \). So 2 and 5\(^2\) must both divide \( |G| \), and we conclude (because 2 and 5\(^2\) are relatively prime) that \( 2 \cdot 5^2 = 50 \) must divide \( |G| \). Of course, the order of \( G \) must then be 50, because the next smallest number that 50 divides is 100, which is larger than the order of \( G \) by hypothesis.

**7.5.20(a)** If \( G \) is an abelian group of order \( 2n \), with \( n \) odd, prove that \( G \) contains exactly one element of order 2.

We have two tasks. First we must show that \( G \) contains at least one element of order 2. Then we must demonstrate that it contains only one such element.

To complete the first task we note that if \( G \) fails to contain at least one order two element, then \( a \neq a^{-1} \) for all \( a \in G \) (because that would imply that \( a^2 = e \) except \( a = e \)). So we list the elements of \( G \) as the set \( G = \{ e, a_1, a_2, \ldots, a_{2n-1} \} \).

It must be that the inverse of \( a_i \) is \( a_j \) for some \( j \neq i \) (because we are assuming that squares are never zero). Because inverses are unique, this means that we can pair off the elements in the set \( \{ a_1, \ldots, a_{2n-1} \} \). This, however, is a contradiction because the cardinality of \( \{ a_1, \ldots, a_{2n-1} \} \) is odd. So it must be that \( G \) has at least one element of order 2.

The second of our two tasks is relatively straightforward. If \( G \) contains more than one element of order two, then it contains a subgroup of order 4. For instance, suppose that \( a, b \in G \) of order 2. Then \( \langle e, a, b, ab \rangle \) is a subgroup of \( G \).
(it is clearly closed, associative, and has an identity–furthermore, \(a^2 = e = b^2\) and \((ab)^2 = abab = aabb = e\), so inverses exist). But if \(G\) has an order 4 subgroup, then \(4 | 2n\) or \(2 | n\). As \(n\) is odd this gives a contradiction.

7.6.24 Let \(H\) be a subgroup of order \(n\) in a group \(G\). If \(H\) is the only subgroup of order \(n\), prove that \(H\) is normal.

Let \(g \in G\). Then it is not hard to see that the set \(gHg^{-1}\) is a subgroup of \(G\). Clearly \(gHg^{-1}\) is nonempty. Similarly, if \(gag^{-1}, gbg^{-1} \in gHg^{-1}\), then \(gag^{-1}(gbg^{-1})^{-1} = gag^{-1}gb^{-1}g^{-1} = gab^{-1}g^{-1}\), so \(gag^{-1}(gbg^{-1})^{-1} \in gHg^{-1}\). Thus \(gHg^{-1}\) is a subgroup of \(G\). But \(gHg^{-1}\) has order \(n\) (here the right coset \(Hg^{-1}\) has order \(n\), and then the left coset \(g(Hg^{-1}) = gHg^{-1}\) also has order \(n\)), and we know that \(H\) is the only subgroup of \(G\) with order \(n\). So \(H = gHg^{-1}\), that is, \(H\) is normal.

7.6.32 If \(N\) is a normal subgroup of order 2 in a group \(G\), prove that \(N \subseteq Z(G)\).

Write \(N = \{e, a\}\) for two elements \(a \neq e \in G\). Then because \(N\) is normal, we know that \(gNg^{-1} = N\) for all \(g \in G\). That means that \(\{geg^{-1}, gag^{-1}\} = gNg^{-1} = N = \{e, a\}\), and because \(geg^{-1} = e\), it must be that \(gag^{-1} = a\). This implies that \(ga = ag\) for all \(g \in G\), which means (by definition) that \(a \in Z(G)\).

The identity is always in the center of \(G\), so we conclude that \(N \subseteq Z(G)\).