Show that every directed path in the subgroup digraph of a cyclic group of order \( N \) has length at most \( \log_2 N \).

Every directed path in such a digraph corresponds to a sequence \( H_0 < H_1 < \cdots < H_r \) of subgroups \( H_i \) in \( G \). The longest path must have \( e = H_0 \) and \( G = H_r \). Let \( p_i = |H_i|/|H_{i-1}| \), so any path for which \( e = H_0 \) and \( G = H_r \) gives a factorization of \( |G| \), and any factorization \( |G| = p_0 \cdots p_r \) gives a path corresponding to subgroups \( H_0 < H_1 < \cdots < H_r \), where \( H_i \) is the unique subgroup of \( G \) of order \( p_0 \cdots p_{i-1} \). Thus the length of the longest path is just the length of the longest factorization \( |G| = p_0 \cdots p_r \). The longest factorization is the one in which each \( p_i \) (except \( p_0 \), since \( p_0 = 1 \)) is prime. If \( n \) is the length of the longest path, we know \( |G| \) is the product of \( n \) primes \( p_1, \ldots, p_n \), and since 2 is the least prime, we have \( 2^n \leq p_1 \cdots p_n = |G| \), or \( n = \log_2 2^n \leq \log_2 |G| \).

(2) Let \( x, g \in S_n \). Assume that \( x = (a_1 \ldots a_r) \) is an \( r \)-cycle. Show that \( gxg^{-1} = (g(a_1) \ldots g(a_r)) \).

For \( 0 \leq i < r \), \( (gxg^{-1})(g(a_i)) = gx(a_i) = g(a_{i+1}) \), so \( gxg^{-1} \) takes \( g(a_i) \) to \( g(a_{i+1}) \), while \( (gxg^{-1})(g(a_r)) = gx(a_r) = g(a_1) \). And if \( z \in \{1, 2, \ldots, n\} - \{g(a_1, \ldots, a_r)\} \), then \( z = g(y) \) for some \( y \), which is not among \( \{a_1, \ldots, a_r\} \), so \( x(y) = y \) and \( (gxg^{-1})(z) = (gxg^{-1})(g(y)) = gxg^{-1}(g(y)) = g(y) = g(y) = z \). This shows that \( gxg^{-1} \) and the cycle \( (a_1) \ldots (a_r) \) permute the elements of \( \{1, \ldots, n\} \) in exactly the same way, so \( gxg^{-1} = (g(a_1) \ldots g(a_r)) \).

(3) Find the centralizer of \((1234)\) in \( S_4 \).

Let \( x = (1234) \) and \( g \in C_{S_4}(x) \). Then \( gx = xg \), hence \( x = gxg^{-1} \). But \( gxg^{-1} = (g(1)g(2) \cdots g(4)) \), so we need \((1234) = (g(1)g(2) \cdots g(4)) \). Since we can write the 4-cycle \((1234)\) in only four different ways (i.e., as any of \((1234) = (2341) = (3412) = (1243)\)), the only thing that \( g \) can do is cyclically permute the numbers \( 1 \) through \( 4 \), \( \text{can't change their relative order (else (g(1)g(2) \cdots g(4)) is not one of the four different ways to write (1234)). But the only cyclic permutations of } 1, 2, 3, 4 \text{ which don't change their relative order is a power of } x, \text{ hence } g \in S_4 \text{. Since } x > C_{S_4}(x), \text{ we see that } C_{S_4}(x) \text{, hence } |C_{S_4}(x)| = |x| = 4. \) Alternatively, it is not hard to use brute force to find \( C_{S_4}(x) \), since \( S_4 \) has only 24 elements.

(4) Let \( n \) and \( N \) be positive integers.

(a) If \( f : Z_n \to Z_N \) is a homomorphism of groups and \( m = f(1) \), show that \( N|m| \) and that \( f(x) = mx \text{ mod } N \), for all \( x \in Z_n \).

(b) Conversely, if \( m \) is a positive integer such that \( N|m| \), show that \( f(x) = mx \text{ mod } N \) defines a homomorphism \( f : Z_n \to Z_N \).

(a) Denote + in the group \( Z_n \) or \( Z_N \) by \( \oplus \), to distinguish it from ordinary addition. Now take the image of \( 1 \oplus \cdots \oplus 1 \) (i.e., \( 1 \) added to itself \( n \) times), keeping in mind that this is the identity in \( Z_n \); i.e., \( 0 = f(0) = f(1 \oplus \cdots \oplus 1) \). Since \( f \) is a homomorphism, this is \( 0 = f(1) \oplus \cdots \oplus f(1) = nf(1) \text{ mod } N = nm \text{ mod } N \). Thus \( N|nm \), since \( nm \) modulo \( N \) is \( 0 \). But we can write any \( x \in Z_n \) as a sum \( 1 \oplus \cdots \oplus 1 \) with itself \( x \) times, so we have \( f(x) = f(1 \oplus \cdots \oplus 1) = f(1) \oplus \cdots \oplus f(1) = mx \text{ mod } N \).

(b) Let \( x, y \in Z_n \) and let \( x + y = qn + r \), with \( 0 \leq r < n \). Then \( f(x + y) = f(r) = mr \text{ mod } N \). But \( f(x) \oplus f(y) = mx + my \text{ mod } N \). Note that \( mx + my - mr = m(x + y) - r = mnq \), hence \( mnq = Nz \) for some \( z \) since \( N|mn \), hence \( mnq = Nz \), so \( mx + my \text{ mod } N = mr \text{ mod } N \). Thus \( f(x + y) = f(x) \oplus f(y) \), so \( f \) is a homomorphism.

(5) Let \( f : G \to H \) be a homomorphism of groups. If \( G \) is finite, show that \( |f(G)| \cdot |\ker f| = |G| \).

Since every element of \( G \) is in \( f^{-1}\{h\} \) for some \( h \in H \), yet inverse images of different elements are disjoint, we see that \( |G| = \sum_{h \in H} |f^{-1}\{h\}| \), but \( |f^{-1}\{h\}| = 0 \) unless \( h \in f(G) \), so \( |G| = \sum_{h \in f(G)} |f^{-1}\{h\}| \). And if \( h = f(g) \), then \( f^{-1}\{h\} = g\ker(f), \) and we know multiplication by an element in a group is injective, so \( |g\ker(f)| = |\ker(f)| \), hence \( |G| = \sum_{h \in f(G)} |f^{-1}\{h\}| = \sum_{h \in f(G)} |\ker(f)| = |f(G)| \cdot |\ker(f)| \).