M417 Homework 6 Spring 2004
Instructions: Solutions are due Fri., March 12.

(1) A *digraph* (i.e., directed graph) is a set of vertices, some of which can be connected by an arrow (i.e., a directed edge). For example, we can associate to each group G its subgroup digraph, in which each subgroup $H \leq G$ is represented by a vertex v_H, and there is an arrow from a vertex v_H to a vertex $v_{H'}$ exactly when H' properly contains H. A *directed path* (of length r) in a digraph is a sequence $v_0, \ldots, v_r$ of vertices such that for each $1 \leq i \leq r$ there is an arrow from v_{i-1} to v_i.

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 $p_0 = |H_0|$, $p_1 = |H_1|/p_0$, ..., $p_r = |H_r|/p_{r-1}$. Then $|G| = p_0 \cdots p_r$, and 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 $p_0 \cdots p_i$. 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 $g, x \in S_n$. 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 $(gxg^{-1})(z) = (gxg^{-1})(g(y)) = gx(y) = g(y) = z$. This shows that gxg^{-1} and the cycle $(g(a_1) \ldots g(a_r))$ 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 $(1234) = (2341) = (3412) = (4123)$), the only thing that g can do is cyclically permute the numbers 1 through 4, it 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 which don't change their relative order is a power of x, hence $g \in < x >$. Since $< x > \subset C_{S_n}(x)$, we see that $< x >= C_{S_4}(x)$, 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 $f : \mathbf{Z}_n \to \mathbf{Z}_N$ is a homomorphism of groups and $m = f(1)$, show that $N|mn$, and that $f(x) = mx \bmod N$, for all $x \in \mathbf{Z}_n$.
   (b) Conversely, if m is a positive integer such that $N|mn$, show that $f(x) = mx \bmod N$ defines a homomorphism $f : \mathbf{Z}_n \to \mathbf{Z}_N$.

(a) Denote $+$ in the group $\mathbf{Z}_n$ or $\mathbf{Z}_N$ 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 $\mathbf{Z}_n$; i.e., $0 = f(0) = f(1 \oplus \cdots \oplus 1)$. Since f is a homomorphism, this is $0 = f(1) \oplus \cdots \oplus f(1) = nf(1) \bmod N = nm \bmod N$. Thus $N|nm$, since nm modulo N is 0. But we can write any $x \in \mathbf{Z}_n$ as a sum $1 \oplus \cdots \oplus 1$ of 1 with itself x times, so we have $f(x) = f(1 \oplus \cdots \oplus 1) = f(1) \oplus \cdots \oplus f(1) = mx \bmod N$.
(b) Let $x, y \in \mathbf{Z}_n$ and let $x + y = qn + r$, with $0 \leq r < n$. Then $f(x \oplus y) = f(r) = mr \bmod N$. But $f(x) \oplus f(y) = mx + my \bmod N$. Note that $mx + my - mr = m(x + y - r) = mqn$, but $mn = Nz$ for some z since $N|mn$, hence $mqn = Nqz$, so $mx + my \bmod N = mr \bmod N$. Thus $f(x \oplus y) = f(x) \oplus f(y)$, 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 $|G| = \Sigma_{h \in H} |f^{-1}(\{h\})|$, but $|f^{-1}(\{h\})| = 0$ unless $h \in f(G)$, so $|G| = \Sigma_{h \in f(G)} |f^{-1}(\{h\})|$. 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

$$|G| = \Sigma_{h \in f(G)} |f^{-1}(\{h\})| = \Sigma_{h \in f(G)} |\ker(f)| = |f(G)| \cdot |\ker(f)|.$$