Part A.

1. Sometimes, the easiest way to prove the equality between two quantities $a = b$ is to find two sets A and B such that A has a elements, B has b elements, and there is a bijection between A and B. This will prove everything that our convention regarding equality requires. In our case, we let A=G/K, $B = G/H \times H/K$ (this is called the *Cartesian product* of G/H and H/K; in other words, B is the set of all ordered pairs (x, y), where $x \in G/H$ and $y \in H/K$). Then A has $|G/K| = i_G(K)$ elements and B has $|G/H| \cdot |H/K| = i_G(H)i_H(K)$ elements. Thus, we only need to find a bijection between A and B. Here is how we do it.

   Choose one element g_x of each right coset $x \in G/H$, and one element h_y of each right coset $y \in H/K$. (*Aside:* It is not at all obvious that we can do it simultaneously for infinitely many cosets. In fact, it is not even possible to either prove or disprove that we can do it, so we just have to assume we can. This is called the *Axiom of Choice.*) Then $x = g_xH$ and $y = h_yK$.

   Consider a function $f : G/H \times H/K \to G/K$ given by $f(x, y) = f(g_xH, h_yK) = g_xh_yK$. We will now prove that f is 1-1 and onto, which will conclude our proof.

   f is 1-1. Let (x, y) and (x', y') be elements of $G/H \times H/K$. Then $x, x' \in G/H$, $y, y' \in H/K$. Suppose that $f(x, y) = f(x'y')$, then $g_xh_yK = g_{x'}h_{y'}K$. Recall that $y = h_yK \subseteq H$ and $y' = h_{y'}K \subseteq H$, so $g_xh_yK \subseteq g_xH = x$ and $g_{x'}h_{y'}K \subseteq g_{x'}H = x'$, hence $x \cap x' \neq \emptyset$, so $x = x'$. But then $g_x = g_{x'}$, so $g_xh_yK = g_{x'}h_{y'}K$ implies $y = h_yK = h_{y'}K = y'$. Thus, $(x, y) = (x', y')$, so f is 1-1.

   f is onto. Let $z \in G/K$, then $z = gK$ for some $g \in z \subseteq G$. But $K \subseteq H$, so $z = gK \subseteq gH$. Thus, z is a subset of some right coset x of H in G. But then $z \subseteq g_xH$, so $(g_x)^{-1}gK = (g_x)^{-1}z \subseteq H$. Hence, $(g_x)^{-1}z = (g_x)^{-1}gK$ is actually a right coset of K in H (not just in G), i.e. $(g_x)^{-1}z = y = h_yK \in H/K$. But then $z = g_xy = g_xh_yK = f(x, y)$, so f is onto.

2. (a) To show $*$ is well defined, we must show that it does not depend on our choice of σ in x. Let $\sigma, \sigma' \in x$, then $x = H\sigma = H\sigma'$, hence $\sigma' = h\sigma$ for some $h \in H$. Then $(H\sigma') * \tau = H\sigma'\tau = Hh\sigma\tau = H\sigma\tau = (H\sigma) * \tau$, so $*$ is well-defined.

   (b) Let $\sigma \in x$ be as in part (a). Then $\tau \in St(x) \iff x * \tau = x \iff H\sigma\tau = H\sigma \iff H\sigma\tau\sigma^{-1} = H \iff \sigma\tau\sigma^{-1} \in H \iff \tau \in \sigma^{-1}H\sigma$. Looking at the first and the last statements, we get $\tau \in St(x) \iff \tau \in \sigma^{-1}H\sigma$, i.e. $St(x) = \sigma^{-1}H\sigma$.

   Let $N = \bigcap_{\sigma \in G} \sigma^{-1}H\sigma$, then any element $\tau \in N$ acts trivially on $H\sigma$ for any $\sigma \in G$, i.e. on any right coset of H in G. Thus, N acts trivially on X.

   (c) *Remark:* The word *action* is actually an algebraic term defined as follows. Let G be a group and let X be a set. An *action* of G on X is a homomorphism from G to $A(X)$. In our problem, we need to show that the right multiplication by elements of G is an action of G on G/H.

   Let $\tau, \rho \in G$, and let $x \in G/H$, $\sigma \in x$, so $x = H\sigma$. Then $(a_\rho \circ a_\tau)(H\sigma) = a_\rho(a_\tau(H\sigma)) = a_\rho(H\sigma\tau) = H\sigma\tau\rho = a_{\tau\rho}(H\sigma)$. Thus, $a_\rho \circ a_\tau = a_{\tau\rho}$. Recall that $a_\rho \circ a_\tau$ means that we apply a_τ first, then a_ρ. Thus, $*$ is a homomorphism from G to $A(X)$, i.e. an action of G on X.

   $\ker(*)$ consists of all elements $\tau \in G$ such that $a_\tau = id_{A(X)}$, i.e. $x * \tau = x$ for all $x \in X$. Thus, $N \subseteq \ker(*)$. On the other hand, if τ acts trivially on X, then $\tau \in \sigma^{-1}H\sigma$ for any right coset $H\sigma \in G/H$, i.e. for any $\sigma \in G$, so $\tau \in \bigcap_{\sigma \in G} \sigma^{-1}H\sigma = N$. Hence, $ker(*) \subseteq N$, so $\ker(*) = N$.

   (d) If $|X| = |G/H| = i_G(H) = n$, then $|A(X)| = n!$ (the product of all positive integers from 1 to n). If $o(G) > n!$, then at least two distinct elements of G have the same image under $*$, i.e. $*(\tau) = *(\rho)$ for some $\tau \neq \rho$ in G. Thus, for any $\sigma \in G$, we have $H\sigma\tau = (H\sigma)*\tau = (H\sigma)*\rho = H\sigma\rho$, i.e. $(H\sigma) * (\tau\rho^{-1}) = H\sigma$ for any $\sigma \in G$, that is $\tau\rho^{-1} \in \ker(*)$. But $\tau\rho^{-1} \neq e$ since $\tau \neq \rho$, so $(e) \neq \ker(*) \lhd G$. Can we have $\ker(*) = G$? If so, then $H\sigma\tau = H\sigma$ for any $\sigma, \tau \in G$, in particular, $H\tau = H$ for any $\tau \in G$, i.e. $\tau \in G \implies \tau \in H$, that is $G \subseteq H \subseteq G$, i.e. $H = G$. Thus, if $H \neq G$, then $\ker(*) \neq G$. This proves $\ker(*)$ is a nontrivial normal subgroup of G.

Part B.

1. Again, as in the Problem A1, the easiest way to show that $a \leq b$ according to our convention is to find two sets A and B such that A has a elements, B has b elements, and there is an injection from A to B or a surjection from B to A. We proceed as in Problem A1.

   Note that H and K are both subgroups of G, so $H \cap K$ is a subgroup of H, of K and of G.

   Let $A = G/(H \cap K)$, $B = G/H \times G/K$. The $|A| = i_G(H \cap K)$, $|B| = |G/H| \cdot |G/K| = i_G(H) i_G(K)$.

   Define a function f from $G/H \times G/K$ to the set of subsets of G as follows. If $x \in G/H$ and $y \in G/K$, let $f(x, y) = x \cap y$. We will show that $G/(H \cap K) \subseteq f(G/H \times G/K)$. Suppose $z \in G/(H \cap K)$. Then $z = g(H \cap K) = gH \cap gK = f(gH, gK)$ for some $g \in G$. Thus, $G/(H \cap K) \subseteq f(G/H \times G/K)$, so $i_G(H \cap K) = |G/(H \cap K)| \leq |f(G/H \times G/K)| \leq |G/H \times G/K| = i_G(H) i_G(K)$.

2. The crucial observation about $S\infty$ is the following. Let M be a positive integer and define $\phi_M : S_M \to S_\infty$ as follows: given $\rho \in S_M$, $\phi_M(\rho) \in S_\infty$ is the permutation such that

$$\phi_M(\rho)(n) = \begin{cases} \rho(n) & \text{if } n \leq M, \\ n & \text{if } n > M. \end{cases}$$

   Then ϕ_M is a monomorphism for any $M \in \mathbb{N}$ (check!). Moreover, for each $\sigma \in S_\infty$, there exists an integer $M > 0$ and a unique permutation $\sigma|_M$ such that $\phi_M(\sigma|_M) = \sigma$. In plain words, to obtain $\sigma|_M \in S_M$ from $\sigma \in S_\infty$, we simply cut off all integers greater than M in the two-line notation of σ. We also see that $S_\infty = \bigcup_{M=1}^{\infty} \phi_M(S_M)$ and $S_M \simeq \phi_M(S_M)$ for any $M \in \mathbb{N}$.

   (a) Let $\sigma, \tau \in S_\infty$. Then there exist some $M_1, M_2 > 0$ such that $\sigma(n) = n$ for $n > M_1$ and $\tau(n) = n$ for $n > M_2$. Let $M = \max(M_1, M_2)$, then $(\sigma\tau)(n) = \sigma(\tau(n)) = \sigma(n) = n$ for $n > M$, so $\sigma\tau \in S_\infty$. Also, if $\sigma(n) = n$ for $n > M$, then $\sigma^{-1}(n) = n$ for $n > M$, so $\sigma^{-1} \in S_\infty$. Therefore, S_∞ is a subgroup of $A(\mathbb{N})$.

   (b) Let $\sigma, \tau \in S_\infty$ and let M be as in part (a). Write σ and τ in cycle notation. Then both σ and τ are products of finitely many finite cycles, hence, of finitely many transpositions, so $\sigma\tau$ is also a product of finitely many transpositions, and $(\sigma\tau)|_M = (\sigma|_M)(\tau|_M)$ (check!). We say that $\sigma \in S_\infty$ is even (respectively, odd) if σ is a product of an even (respectively, odd) number of transpositions. Moreover, if M is such that $\sigma(n) = n$ for $n > M$, then σ is even in S_∞ if and only if $\sigma|_M$ is even in S_M. Since even permutations are well-defined in S_M for any $M > 0$ (i.e. in any representation of a permutation in S_M as a product of transpositions, the number of these transpositions has the same parity), it follows that even permutations are well-defined in S_∞. Together with $(\sigma\tau)|_M = (\sigma|_M)(\tau|_M)$, this means a product $\sigma\tau$ is even (respectively, odd) if both σ and τ are even (respectively, if one of σ or τ is even and the other is odd).

   Furthermore, if $\sigma, \tau \in S_\infty$ and M is as in part (a), then $(\tau^{-1}\sigma\tau)|_M = (\tau^{-1})|_M(\sigma|_M)(\tau|_M)$, so $(\tau^{-1}\sigma\tau)|_M$ is even if and only if $\sigma|_M$ is even, i.e. $\tau^{-1}\sigma\tau$ is even if and only if σ is even. Thus, $\tau^{-1} A_\infty \tau \subseteq A_\infty$ for any $\tau \in S_\infty$, i.e. $A_\infty \lhd S_\infty$.

   Moreover, if $\tau \in S_\infty - A_\infty$, i.e. if τ is odd, then $\tau(12)$ is even, i.e. $\tau(12) \in A_\infty$, that is $\tau \in A_\infty(12)$. Thus, there are only 2 right cosets of A_∞ in S_∞, namely, A_∞ and $A_\infty(12)$, so $(S_\infty : A_\infty) = 2$.

   (c) Suppose A_∞ has a normal subgroup N. Let $n \in \mathbb{N}$ and consider $\phi_n(A_n) \cap N$ (this is a subgroup of N which consists of all even permutations which fix all elements greater than n). We have $y^{-1}Ny \subseteq N$ for any $y \in S_\infty$, hence, $y^{-1}Ny = N$ for any $y \in \phi_n(A_n)$, so $y^{-1}(\phi_n(A_n) \cap N)y = y^{-1}\phi_n(A_n)y \cap y^{-1}Ny = \phi_n(A_n) \cap N$ for any $y \in \phi_n(A_n)$, in other words, $\phi_n(A_n) \cap N \lhd \phi_n(A_n)$. But $\phi_n(A_n) \simeq A_n$ and A_n is simple for $n \geq 5$, so $\phi_n(A_n)$ is also simple. Thus, $\phi_n(A_n) \cap N$ is either (e) or A_n, i.e. for each $n \geq 5$, either $\phi_n(A_n) \cap N = (e)$ or $\phi_n(A_n) \subseteq N$. Note that permutations in A_n which fix n may actually be thought of as permutations in A_{n-1}, in other words, $\phi_{n-1}(A_{n-1}) \subseteq \phi_n(A_n)$ for any n. If for some $n \geq 5$, we have $\phi_n(A_n) \subseteq N$, then for any $m > n$, we have $(e) \neq \phi_n(A_n) \subseteq \phi_m(A_m) \cap N$, so $\phi_m(A_m) \subseteq N$. Note that $A_\infty = \bigcup_{n=1}^{\infty} \phi_n(A_n) = \bigcup_{n=5}^{\infty} \phi_n(A_n)$, so we have two possibilities. Either $\phi_n(A_n) \cap N = (e)$ for

all $n \geq 5$, so $N = A_\infty \cap N = \bigcup_{n=5}^{\infty} (\phi_n(A_n) \cap N) = \bigcup_{n=5}^{\infty} (e) = (e)$, or there is $n \geq 5$ such that $\phi_m(A_m) \subseteq N$ so all $m \geq n$, so $N = A_\infty \cap N = \bigcup_{n=5}^{\infty} (\phi_n(A_n) \cap N) = \bigcup_{n=5}^{\infty} \phi_n(A_n) = A_\infty$. Thus, if $N \lhd A_\infty$, then $N = (e)$ or $N = A_\infty$, so A_∞ is simple.

(d) Clearly, $(S_\infty : S_\infty) = 1$. Also, $(S_\infty : A_\infty) = 2$ from part (b), so S_∞ and A_∞ are two subgroups of finite index in S_∞.

Now suppose $N \lhd S_\infty$ and $(S_\infty : N)$ is finite. Then $N \cap A_\infty \lhd A_\infty$. But A_∞ is simple, so $N \cap A_\infty = A_\infty$ or $N \cap A_\infty = (e)$. In the first case, $A_\infty \subseteq N$, hence A_∞ is a subgroup of N, so $1 \leq (S_\infty : N) \leq (S_\infty : A_\infty) = 2$. If $(S_\infty : N) = 1$, then $N = S_\infty$. Since N contains all even permutations, it follows that $N = S_\infty$ (i.e. $(S_\infty : N) = 1$) if N contains any odd permutation. Thus, $(S_\infty : N) = 2$ implies that N contains no odd permutations, so $N = A_\infty$. Suppose $N \cap A_\infty = (e)$. Since $(S_\infty : N)$ is finite and S_∞ is infinite, N must be infinite. Thus, there is an element $a \in N$, $a \neq e$. Then $a \notin A_\infty$, i.e. a is an odd permutation. But a^2 is even, so $a^2 = e$. If N has at least 2 distinct elements other than e, say a, b, then ab is even, so $ab = e$. But then $a^2 = e = ab$, so $a = b$. Thus, N may contain at most one element other than e. But N is infinite. Contradiction. Thus, $N \cap A_\infty \neq (e)$, so $N = S_\infty$ or $N = A_\infty$.

On the other hand, consider any cyclic subgroup generated by a cycle with n elements, then this cyclic subgroup has order n. Since there are infinitely many ways to choose n elements from $\mathbb{N}$, S_∞ has infinitely many subgroups of exact order n for any $n \in \mathbb{N}$.

(e) Recall that every finite group of n elements is isomorphic to a subgroup of S_n, hence, via the isomorphism ϕ_n, to a subgroup of $\phi_n(S_n)$, which in turn is a subgroup of S_∞. Therefore, any finite group is isomorphic to a subgroup of S_∞.

(f) Up to an isomorphism, $\mathbb{Z}$ is *the* infinite cyclic group. In other words, if $A = (a)$ has infinitely many elements, then $A = \{a^n \mid n \in \mathbb{Z}\}$.

Suppose that $\mathbb{Z} = (1)$ (the infinite cyclic group generated by 1) is isomorphic to a subgroup of S_∞. Then there is a monomorphism $f : \mathbb{Z} \hookrightarrow S_\infty$. ("$\hookrightarrow$" denotes injection.) Then $f(1) \in S_\infty$ must be an element of infinite order. But any permutation in S_∞ is in a finite subgroup $\phi_n(S_n) \simeq S_n$ for some $n > 0$, hence, is of finite order. Thus, there is no monomorphism from $\mathbb{Z}$ to S_∞.

In fact, we have proven much more: no group which has elements of infinite order is isomorphic to a subgroup of S_∞. Recall that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is of infinite order in $SL(2, \mathbb{Z})$ since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for any $n \in \mathbb{Z}$ (recall Problem B3, Assignment 2). Therefore, $SL(2, \mathbb{Z})$ is not isomorphic to any subgroup of S_∞.

(g) Let H be a finitely generated subgroup of S_∞, and let $\tau_1, \ldots, \tau_n$ be its generators. Then, for each $k = 1, \ldots, n$, there exists $M_k > 0$ such that $\tau_k(n) = n$ any $n \geq M_k$. Let $M = \max(M_1, \ldots, M_k)$. Then $\tau_k(n) = n$ for any $n \geq M$ and any $k = 1, \ldots, n$. Thus, $\tau_1, \ldots, \tau_k \in \phi_M(S_M)$, so $H \subseteq \phi_M(S_M)$ since $\phi_M(S_M)$ is a subgroup of S_∞. But $\phi_M(S_M)$ is finite (it has $M!$ elements), so H is finite as well.

3. (a) Suppose $\phi : G \to G$ is an automorphism of a finite group G such that its only fixed point is 1. Consider a function $f : G \to G$ defined by $f(y) = y^{-1}\phi(y)$. We will show that f is a bijection.

Suppose $f(y) = f(z)$ for some $y, z \in G$, then $y^{-1}\phi(y) = z^{-1}\phi(z)$, so $zy^{-1} = \phi(z)\phi(y)^{-1} = \phi(zy^{-1})$. Hence, zy^{-1} is a fixed point of ϕ, so $zy^{-1} = 1$, i.e. $z = y$. Therefore, f is 1-1.

Since f is 1-1, we have $|f(G)| = |G|$ (thinking of G as the domain on both sides). But G is also the target set and G is *finite*, so f must be a bijection, hence, onto.

Thus, for every $x \in G$ there exists a unique $y \in G$ such that $x = f(y) = y^{-1}\phi(y)$, i.e. such that $yx = \phi(y)$.

Now suppose, in addition, that ϕ^2 is the identity map on G, i.e. $\phi(\phi(g)) = g$ for any $g \in G$. Let $x \in G$, and let $y \in G$ be such that $yx = \phi(y)$. Then $y = \phi(\phi(y)) = \phi(yx) = \phi(y)\phi(x) = yx\phi(x)$, so $x\phi(x) = 1$ for any $x \in G$. Thus, $\phi(x) = x^{-1}$ for any $x \in G$. Let $a, b \in G$, then $\phi(ab) = \phi(a)\phi(b)$ is equivalent to $(ab)^{-1} = a^{-1}b^{-1} = (ba)^{-1}$, i.e. $ab = ba$. Thus, any two elements of G commute, so G is abelian.