Part A.

1. (a) For any element $a \in N(H)$, we have $a^{-1}Ha = H$, hence $H \lhd N(H)$.

   (b) If K is a subgroup of G such that $H \lhd K$, then for any $k \in K$, $k^{-1}Hk = H$, so $k \in N(H)$. Therefore, $K \subseteq N(H)$. Since K is a group, we have $K \leq N(H)$.

   (c) We have $g \in stab(H) \iff g \cdot H = H \iff gHg^{-1} = H \iff g \in N(H)$, hence $stab(H) = N(H)$. Now the orbit of H is the set $orb(H) = \{g \cdot H \mid g \in G\} = \{gHg^{-1} \mid g \in G\}$, in other words, the set of all subgroups conjugate to H. Hence, by the orbit-stabilizer theorem, the number of subgroups of H conjugate to H is $|orb(H)| = |G : stab(H)| = |G : N(H)|$.

Part B.

1. We know from earlier homework that S_n is generated by the set of transpositions of consecutive elements. Thus, we only need to prove that the cycles (12) and $(123 \ldots n)$ generate all transpositions $(i\ i+1)$. Let us prove by induction on i that

$$(i\ i+1) = (1\ 2\ 3 \ldots n-1\ n)^{i-1}(1\ 2)(1\ 2\ 3 \ldots n-1\ n)^{-(i-1)}$$

for any $1 \leq i \leq n-1$. Clearly, our claim is true for $i = 1$. Suppose it is true for some $1 \leq i < n-1$. Let us prove that it is true for $(i\ i+1)$ as well. It is easy to see that we only need to prove that

$$(i+1\ i+2) = (1\ 2\ 3 \ldots n-1\ n)(i\ i+1)(1\ 2\ 3 \ldots n-1\ n)^{-1}.$$

Let $\tau = (123 \ldots n)$, $\sigma_i = (i\ i+1)$ and define, for the purposes of this problem only, $n+1 := 1$ and $0 := n$. Thus, we need to prove that $\sigma_{i+1} = \tau\sigma_i\tau^{-1}$. Note that $\tau(j) = j+1$ for all j, so $\tau^{-1}(j) = j-1$ for all j. Suppose that $j \notin \{i+1, i+2\}$, then $j-1 \notin \{i, i+1\}$, so $\sigma_i(j-1) = j-1$. Therefore, $\tau\sigma_i\tau^{-1}(j) = \tau\sigma_i(j-1) = \tau(j-1) = j$. Hence, the only elements that may be moved by $\tau\sigma_i\tau^{-1}$ are $i+1$ and $i+2$. Now we have $\tau\sigma_i\tau^{-1}(i+1) = \tau\sigma_i(i) = \tau(i+1) = i+2$ and $\tau\sigma_i\tau^{-1}(i+2) = \tau\sigma_i(i+1) = \tau(i) = i+1$. Thus, $\tau\sigma_i\tau^{-1}(j) = \sigma_{i+1}(j)$ for all $j = 1, 2, \ldots, n$, so $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$, which ends the proof.

2. (a) Let $[h, k] \in \Delta(G)$ and $g \in G$, then

$$\begin{aligned}[ghg^{-1}, gkg^{-1}] &= (ghg^{-1})(gkg^{-1})(ghg^{-1})^{-1}(gkg^{-1})^{-1} \\ &= ghg^{-1}gkg^{-1}gh^{-1}g^{-1}gk^{-1}g^{-1} = ghkh^{-1}k^{-1}g^{-1} = g[h, k]g^{-1},\end{aligned}$$

   so for any $[h, k] \in \Delta(G)$ and any $g \in G$, $g[h, k]g^{-1} \in \Delta(G)$.

   It is easy to check that . Since $\Delta(G)$ is the subgroup generated by all commutators of elements of G, and $[h, k]^{-1} = [k, h]$ (easy to check), we get that any element of $d = \Delta(G)$ is a product of finitely many commutators, i.e. $d = c_1c_2 \ldots c_m$ for some commutators $c_1, c_2, \ldots, c_m$ of elements of G. But then $gdg^{-1} = gc_1c_2 \ldots c_mg^{-1} = (gc_1g^{-1})(gc_2g^{-1}) \ldots (gc_mg^{-1}) \in \Delta(G)$ since each $gc_ig^{-1} \in \Delta(G)$ as we proved. Hence, $g\Delta(G)g^{-1} \subseteq \Delta(G)$ for any $g \in G$, and thus $\Delta(G) \lhd G$.

(b) We have that $(gh)^{-1}(hg) = h^{-1}g^{-1}hg = [h^{-1}, g^{-1}] \in \Delta(G)$, so $gh\Delta(G) = hg\Delta(G)$ for any $g, h \in G$. But then we have

$$(g\Delta(G))(h\Delta(G)) = gh\Delta(G) = hg\Delta(G) = (h\Delta(G))(g\Delta(G)),$$

for any two cosets $g\Delta(G)$ and $h\Delta(G)$ in $G/\Delta(G)$, and thus $G/\Delta(G)$ is an abelian group.

Part C.

1. For $\sigma \in G$, we have $\sigma = \begin{bmatrix} 1/c & b \\ 0 & c \end{bmatrix}$ for some $c > 0$ and some real b. Let $(x, y) \in \mathbb{R}^2$. From the definition of the action of G on $\mathbb{R}^2$, it is clear that the action of any $\sigma \in G$ preserves the sign of y, and if $y = 0$ then the action of any $\sigma \in G$ preserves the sign of x.

   If $y > 0$, then
   $$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1/y & x \\ 0 & y \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}; \qquad \begin{bmatrix} 1/c & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ c \end{bmatrix}, \quad c > 0.$$
   If $y < 0$, then
   $$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1/y & -x \\ 0 & -y \end{bmatrix} \begin{bmatrix} 0 \\ -1 \end{bmatrix}; \qquad \begin{bmatrix} 1/c & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 0 \\ -1 \end{bmatrix} = \begin{bmatrix} -b \\ -c \end{bmatrix}, \quad -c < 0.$$
   If $y = 0$ and $x > 0$, then
   $$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & 1/x \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}; \qquad \begin{bmatrix} a & b \\ 0 & 1/a \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ 0 \end{bmatrix}, \quad a > 0.$$
   If $y = 0$ and $x < 0$, then
   $$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} -x & 0 \\ 0 & -1/x \end{bmatrix} \begin{bmatrix} -1 \\ 0 \end{bmatrix}; \qquad \begin{bmatrix} a & b \\ 0 & 1/a \end{bmatrix} \begin{bmatrix} -1 \\ 0 \end{bmatrix} = \begin{bmatrix} -a \\ 0 \end{bmatrix}, \quad -a < 0.$$
   If $y = 0$ and $x = 0$, then
   $$\begin{bmatrix} a & b \\ 0 & 1/a \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$
   Thus,

   - the upper half-plane, $y > 0$, is the orbit of $(0, 1)$;
   - the lower half-plane, $y < 0$, is the orbit of $(0, -1)$;
   - the positive x-axis, $y = 0$ and $x > 0$, is the orbit of $(1, 0)$;
   - the negative x-axis, $y = 0$ and $x < 0$, is the orbit of $(-1, 0)$;
   - the origin, $(0, 0)$, is in a separate orbit by itself.

   Altogether, there are 5 orbits.

2. If G is a finite group, then H is also finite, so by Lagrange theorem, $|G : H| = |G|/|H|$, $|H : K| = |H|/|K|$ and $|G : K| = |G|/|K|$, so obviously $|G : K| = |G : H||H : K|$.

   The proof for any group G, finite or infinite, is less obvious. However, the advantage of this proof is that it also applies to the case when either or both of $|G : H|$ and $|H : K|$ are not necessarily finite.

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, and let B be the set of all ordered pairs (x, y), where $x \in G/H$ and $y \in H/K$ (so, in fact, B is the external direct product $G/H \oplus H/K$). Then $|A| = |G/K| = |G : K|$ and $|B| = |G/H||H/K| = |G : H||H : K|$, so we only need to find a bijection between A and B. Here is how we do it.

Choose *one* element g_x of each left coset $x \in G/H$, and *one* element h_y of each left 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 $x = g_x H$ and $y = h_y K$.

Consider a function $f : G/H \oplus H/K \to G/K$ given by $f(x, y) = f(g_x H, h_y K) = g_x h_y K$. 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 $G/H \oplus H/K$. Then $x, x' \in G/H$, $y, y' \in H/K$. Suppose that $f(x, y) = f(x'y')$, then $g_x h_y K = g_{x'} h_{y'} K$. Recall that $y = h_y K \subseteq H$ and $y' = h_{y'} K \subseteq H$, so $g_x h_y K \subseteq g_x H = x$ 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 $g_x h_y K = g_{x'} h_{y'} K$ implies $y = h_y K = h_{y'} K = y'$. 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 left coset x of H in G. But then $z \subseteq g_x H$, so $(g_x)^{-1} gK = (g_x)^{-1} z \subseteq H$. Hence, $(g_x)^{-1} z = (g_x)^{-1} gK$ is actually a left coset of K in H (not just in G), i.e. $(g_x)^{-1} z = y = h_y K \in H/K$. But then $z = g_x y = g_x h_y K = f(x, y)$, so f is onto.