**Math 301** **Sketch of Solutions for Homework 5**

**Part A.**

1. Consider a map $\phi : \mathbb{Z} \to SL(2,\mathbb{Z})$ given by $\phi(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. Then it is easy to check that $\phi$ is 1-1 and $\phi(m)\phi(n) = \phi(m+n)$ so $\phi$ is a monomorphism. Hence, $\phi(\mathbb{Z})$ is a subgroup of $SL(2,\mathbb{Z})$, and $\phi : \mathbb{Z} \to \phi(\mathbb{Z})$ is a homomorphism which is 1-1 and onto, i.e. an isomorphism. Therefore, $\mathbb{Z}$ is isomorphic to a subgroup of $SL(2,\mathbb{Z})$.

2. Not all permutations of order 6 in $S_6$ cyclic. For example, $(12)(345)(6)$ is of order $\text{lcm}(2,3,1) = 6$ and is a product of three disjoint cycles, so it's not cyclic.

3. Every permutation can be written as a product of 2-cycles. Suppose $\alpha = \rho - 1\rho_2 \dots \rho_s$ and $\beta = \tau_1\tau_2 \dots \tau_t$, where each $\rho_i$ and $\tau_j$ is a 2-cycle, then $\beta^{-1} = \tau_t^{-1} \dots \tau_2^{-1}\tau_1^{-1} = \tau_t \dots \tau_2\tau_1$ (since $\tau^{-1} = \tau$ for any 2-cycle $\tau$). Hence, $\alpha$ is a product of $s$ 2-cycles and $\beta\alpha\beta^{-1}$ is a product of $t + s + t = s + 2t$ 2-cycles. The integers $s$ and $s + 2t$ differ by an even integer $2t$, hence $s$ and $s + 2t$ are either both even or both odd, so $\alpha$ and $\beta\alpha\beta^{-1}$ are either both even or both odd.

4. (a) Let us prove that $stab(x)$ is a subgroup of $G$ for any $x \in X$. Let $\pi, \sigma \in stab(x)$, then $\pi(x) = x$ and $\sigma(x) = x$, so $(\pi\sigma)(x) = \pi(\sigma(x)) = \pi(x) = x$, i.e. $\pi\sigma \in stab(x)$. Similarly, applying $\pi^{-1}$ to both sides of the first equation, we get $x = \pi^{-1}(x)$, i.e. $\pi^{-1} \in stab(x)$. Since this is true for any $\pi, \sigma \in stab(x)$, it follows that $stab(x)$ is a subgroup of $G$.

   (b) For the identity permutation $id_X = e_G$, we have $id_X(x) = x$ for every $x \in X$, so $x \sim x$ for every $x \in X$. Therefore, $\sim$ is reflexive.

   For any $x, y \in X$, if $x \sim y$, then $x = \pi(y)$ for some $\pi \in G$, so $y = \pi^{-1}(x)$ and $\pi^{-1} \in G$, hence $y \sim x$. Therefore, $\sim$ is symmetric.

   For any $x, y, z \in x$, if $x \sim y$ and $y \sim z$, then $x = \pi(y)$ and $y = \sigma(z)$ for some $\pi, \sigma \in G$, so $x = \pi(\sigma(z)) = (\pi\sigma)(z)$ and $\pi\sigma \in G$, hence $x \sim z$. Therefore, $\sim$ is transitive.

   Thus, $\sim$ is an equivalence relation, so the action of $G$ partitions $X$ into disjoint orbits.

**Part B.**

1. Let us prove that $S_n$ is generated by transpositions of consecutive integers. We know that $S_n$ is generated by all transpositions (2-cycles), so we only need to prove that every transposition $(ij)$ is a product of transpositions of consecutive integers. Since $(ji) = (ij)$, assume without loss of generality that $i < j$. We will give a proof by induction on $j - i$. If $j - i = 1$, then $(ij) = (i\ i+1)$, so our assertion is true. Assume our assertion is true for all $(i'j')$ with $j' - i' \leq k$, $k \geq 1$, i.e. $(i'j')$ is a product of transpositions of consecutive integers if $j' - i' \leq k$. Consider any $(ij)$ with $j - i = k + 1$. Then $(i\ i+1)(i+1\ j)(i\ i+1)$ and $j - (i+1) = j - i - 1 \leq k$, so $(i+1\ j)$ is a product of transpositions of consecutive integers, and hence, so is $(ij)$. Thus, by induction, we obtain that any $(ij) \in S_n$ is a product of transpositions of consecutive integers, so $S_n$ is generated by the set $\{(12), (23), (34), \dots, (n-1\ n)\}$.

2. Prove that $D_{12}$ and $S_4$ are not isomorphic (even though they have the same number of elements).

   The group $D_{12}$ has an element of order 12. Any element in $S_4$ is a product of disjoint cycles whose lengths sum to 4. Now it is easy to check that if $l_1 + \dots + l_k = 4$ for some positive integers $l_i$, $i = 1, \dots, k$, then $k \leq 4$ and $\text{lcm}(l_1, \dots, l_k) \neq 12$ (the possible choices are: $1,1,1,1$; $2,1,1$; $2,2$; $3,1$; $4$ with lcm's $1, 2, 2, 3, 4$).

3. Any permutation in $A_n$ can be expressed as a product of an even number of 2-cycles, say $2k$ 2-cycles. Break these two-cycles into $k$ pairs of consecutive 2-cycles. Each pair has 0 or 1 or 2 elements in common. If the 2-cycles in the same pair have 2 elements in common, then we have $(ab)(ab) = \epsilon = (abc)(acb)$. If the 2-cycles in the same pair have 1 element in common, then we have $(ab)(ac) = (acb)$.

If the 2-cycles in the same pair have 0 elements in common, then we have $(ab)(cd) = (abc)(adc)$. (Of course, $a, b, c, d$ are all distinct.) Thus, a product of two 2-cycles can be written as a product of one or two 3-cycles, so any permutation in $A_n$ is a product of 3-cycles, and hence $A_n$ is generated by 3-cycles.

**Part C.**

1. Write each cyclic permutation so that the cycle ends on $n$. Then we can write any cyclic permutation in $S_n$ as $(\pi n)$, where $\pi$ is any permutation in $S_{n-1}$ written in one-line notation. Obviously, $(\pi_1 n) = (\pi_2 n)$ if and only if $\pi_1 = \pi_2$, so the number of cyclic permutations in $S_n$ is equal to the order of $S_{n-1}$, i.e. $(n-1)!$.

2. Let us prove that all permutations of order $n$ in $S_n$ are cyclic if and only if $n$ is a power of a prime number.

   Any integer $n$ can be written as $n = p_1^{i_1} \dots p_r^{i_r}$ for some positive integers $r$, $i_1, \dots, i_r$, and some prime numbers $p_1, \dots, p_r$. Note that $p_1^{i_1} \dots p_r^{i_r} = \mathrm{lcm}(p_1^{i_1}, \dots, p_r^{i_r})$. Since powers of different prime numbers are relatively prime to each other.

   (ONLY IF) Suppose that $r > 1$. Consider a permutation $\pi = c_1 c_2 \dots c_r c_{r+1} \dots c_k$, $k = n - (p_1^{i_1} + \dots + p_r^{i_r})$, where $c_j$'s are disjoint cycles, and $c_j$ is of length $p_j^{i_j}$ for $j \le r$, and of length 1 if $j > r$. Clearly, $|\pi| = \mathrm{lcm}(|c_1|, \dots, |c_k|) = \mathrm{lcm}(p_1^{i_1}, \dots, p_r^{i_r}, 1, \dots, 1) = p_1^{i_1} \dots p_r^{i_r} = n$, but $\pi$ has at least $r > 1$ cycles, so $\pi$ is not cyclic.

   (IF) Now suppose $r = 1$, i.e. $n = p^i$ for some prime $p > 0$ and some integer $i \ge 0$. Any $\pi \in S_n$ can be written a product of disjoint cycles, say $\pi = c_1 \dots c_m$. Then $p^i = |\pi| = \mathrm{lcm}(|c_1|, \dots, |c_m|)$. Note that the highest power of $p$ that divides $\mathrm{lcm}(|c_1|, \dots, |c_m|)$ is the highest power of $p$ that divides at least one of $|c_1|, \dots, |c_m|$. Thus, $p^i$ must divide some $|c_j|$. But $1 \le |c_j| \le |\pi| = p^i$, and the only integer between 1 and $p^r$ divisible by $p^i$ is $p^i$. Therefore, $|c_j| = p^i$, so $\pi = c_i$, and hence $\pi$ is cyclic.