HW3

Please type or photograph your solution and turn it into a pdf before submitting it to Canvas. The first two problems will be graded for correctness.

1. Recall that by S_n we mean the permutation group of $\{1, 2, \ldots, n\}$.
   (a) Find all the automorphisms of S_2.
   (b) Find all the automorphisms of S_3.

   Hint: If $f : G \to G$ is a group isomorphism, $g \in G$, then $g^n = e$ iff $f(g)^n = e$, because $f(g)^n = f(g^n)$ and f is a bijection that sends the identity e to itself.

2. Let G be a group, $f : G \to G$ a function, and $\sim$ an equivalence relation on G. Let $G \times G$ be the direct product of G with itself, i. e. with group operation defined as $((a, b), (c, d)) \mapsto (ac, bd)$
   (a) Show that $G_f = \{(g, f(g)) : g \in G\}$ is a subgroup of $G \times G$ iff f is a group homomorphism.
   (b) Show that $G_\sim = \{(a, b) \in G \times G : a \sim b\}$ is a subgroup of $G \times G$ iff there is a normal subgroup H of G, such that $\sim = \{(a, b) \in G \times G : b^{-1}a \in H\}$.

3. Let G be a group, S a subset of G. For every $g \in G$, define S^g as $S^g = \{gsg^{-1} : s \in S\}$. Suppose for every $g \in G$, $S^g \subseteq S$, show that for every $g \in G$, $S^g = S$.

4. Let G be a group, S a subset of G. Let H_S be a subset of G consisting of identity e together with all elements of the form $s_1 s_2 \ldots s_n$, where each s_j is either in S or its inverse is in S. Show that H_S is a subgroup of G, and any subgroup of G containing all elements in S must have H_S as a subgroup, i. e. $H_S = \langle S \rangle$

5. Recall that if group G satisfies $G = \langle S \rangle$, we say S is a generating set of G. Let $n > 2$ be an integer.
   (a) Let S be a finite subset of $(\mathbb{Q}, +)$, show that $\langle S \rangle \neq \mathbb{Q}$.
   (b) Show that S_n, which is the group of bijections from $\{1, \ldots, n\}$ to itself, with group operation being the composition, has a generating set with no more than $n - 1$ elements.

(c) Write down a generating set of S_n with only two elements.

Answer:

1. (a) S_2 has only 2 elements and any group homomorphism sends identity to identity, hence if it is also bijective it has to be id_{S_2}.

   (b) Let the 6 elements of S_3 be $\sigma_0 = id_{\{1,2,3\}}$, $\sigma_1 = \{(1,2),(2,1),(3,3)\}$, $\sigma_2 = \{(1,3),(3,1),(2,2)\}$, $\sigma_3 = \{(2,3),(3,2),(1,1)\}$, $\sigma_4 = \{(1,2),(2,3),(3,1)\}$, $\sigma_5 = \{(1,3),(3,2),(2,1)\}$. Then by the hint, any automorphism must permute the three elements σ_1, σ_2 and σ_3. On the other hand, $\sigma_4 = \sigma_2\sigma_1$, $\sigma_5 = \sigma_3\sigma_1$, so an automorphism is determined by its value on σ_1, σ_2 and σ_3. The six inner automorphisms $x \mapsto gxg^{-1}$ where $g \in S_3$ provides all the possible permutations of $\{\sigma_1, \sigma_2, \sigma_3\}$, hence they are all the automorphisms of S_3.

2. (a) Assume $G_f \leq G\times G$. For any $a, b \in G$, $(a, f(a)), (b, f(b)) \in G_f$, hence their product, $(ab, f(a)f(b)) \in G_f$, which implies that $f(a)f(b) = f(ab)$, i.e. $f \in Hom(G, G)$.

   If $f \in Hom(G, G)$, then $f(e) = e$, hence $(e, e) = (e, f(e)) \in G_f$. Let $(a, f(a)), (b, f(b))$ be any two elements of G_f, then their product in $G \times G$, $(ab, f(a)f(b)) = (ab, f(ab)) \in G_f$, and $(a, f(a))^{-1} = (a^{-1}, f(a)^{-1}) = (a^{-1}, f(a^{-1})) \in G_f$. So $G_f \leq G \times G$.

   (b) Assume $G_\sim \leq G_\sim$. Let $H = [e]$, we first show that H is a normal subgroup of G:

      i. $e \sim e$ hence $e \in H$.

      ii. If $a, b \in H$, $(a, e), (b, e) \in G_\sim$, hence $(ab, e) \in G_\sim$, which implies that $ab \in H$.

      iii. If $a \in H$, $(a, e) \in G_\sim$, hence $(a, e)^{-1} = (a^{-1}, e) \in G_\sim$, which implies that $a^{-1} \in H$.

      iv. If $a \in H$, $g \in G$, then $(a, e), (g, g), (g^{-1}, g^{-1}) \in G_\sim$, hence $(g, g)(a, e)(g^{-1}, g^{-1}) = (gag^{-1}, e) \in G_\sim$, which implies that $gHg^{-1} \subseteq H$. Now apply the conclusion of Problem 3.

   Now $(a, b) \in \sim$ iff $(a, b) \in G_\sim$ iff $(b^{-1}, b^{-1})(a, b) \in G_\sim$ iff $b^{-1}a \in H$.

3. By assumption, for every $s \in S$, $g^{-1}s(g^{-1})^{-1} = g^{-1}sg \in S$, hence $s = g(g^{-1}sg)g^{-1} \in S^g$, which implies that $S = S^g$.

4. By construction, H_S contains identity, and is closed under multiplication as well as inverse ($(s_1 \dots s_n)^{-1} = s_n^{-1} \dots s_1^{-1}$), hence is a subgroup of G that contains S. Any subgroup of G containing S must also contain the elements of S, their inverses and their finite products, hence it is the smallest such subgroup, $H_S = \langle S \rangle$.

5. (a) Let $S = \{p_1/q_1, \dots, p_n/q_n\}$ where $p_i, q_i \in \mathbb{Z}$, then $1/2 \prod_n q_n \notin \langle S \rangle$ because $\langle S \rangle$ consists of finite sums or differences of p_i/q_i by Problem 4, which can always be written as $p/lcm(q_1, \dots, q_n)$.

(b) Let σ_i be the element in S_n which switches i and $i+1$ and keeps the other numbers the same. We will now show that $S_n = \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$. Given $g \in S_n$, let $k(g)$ be the largest natural number such that $g(i) = i$ for all $i > k(g)$. We shall use induction to show that all g such that $k(g) \leq n$ lies in $\langle \sigma_1, \ldots, \sigma_{n-1} \rangle$

i. If $k(g) = 0$, $g = e \in \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$

ii. Suppose all g' with $k(g') < k$ are in $\langle \sigma_1, \ldots, \sigma_{n-1} \rangle$. Let $g \in S_n$, $k(g) = k+1$, then $g(k+1) < k+1$, $(\sigma_k \sigma_{k-1} \ldots \sigma_{g(k+1)} g)(k+1) = k+1$, hence $\sigma_k \sigma_{k-1} \ldots \sigma_{g(k+1)} g \in \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$ by inductive hypothesis, which implies that $g \in \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$.

(You may recognize that what I wrote here is basically Selection Sort. You can prove this via other sorting algorithms as well.)

(c) One element can be σ_1, and the other element can be chosen as the one sending 1 to 2, 2 to 3, etc, n to 1, which we denote as τ. By Part (b) above, any element in S_n can be written as a finite product of the σ_is, and $\sigma_i = \tau^{i-1} \sigma_1 \tau^{1-i}$.