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.

1.

Solution

(a). $$S_2 = \left\{ \underbrace{\begin{matrix} 1 \to 1 \\ 2 \to 2 \end{matrix}}_{=p_1},\ \underbrace{\begin{matrix} 1 \to 2 \\ 2 \to 1 \end{matrix}}_{=p_2} \right\}$$

if $f \in \mathrm{Aut}(S_2)$ $\left.\begin{matrix} f(p_1) = p_1 \\ f(p_2) = p_2 \end{matrix}\right\}$ is a trivial homomorphism.

$\left.\begin{matrix} f(p_1) = p_2 \\ f(p_2) = p_1 \end{matrix}\right\}$ doesn't send the identity (p_1) to itself. so it's not a homomorphism.

$$\mathrm{Aut}(S_2) = \{ f : x \mapsto x \}$$

(b) $$S_3 = \left\{ \underbrace{\begin{matrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{matrix}}_{=p_1},\ \underbrace{\begin{matrix} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{matrix}}_{=p_2},\ \underbrace{\begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{matrix}}_{=p_3},\ \underbrace{\begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix}}_{=p_4},\ \underbrace{\begin{matrix} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{matrix}}_{=p_5},\ \underbrace{\begin{matrix} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{matrix}}_{=p_6} \right\} \quad (*)$$

If $f \in \mathrm{Aut}(S_3)$. then $p_1 = e \Rightarrow f(p_1) = e = p_1$

$p_2^2 = e \Rightarrow f^2(p_2) = e \Rightarrow f(p_2) \in \{p_2, p_3, p_6\}$

$p_3^2 = e \Rightarrow f^2(p_3) = e \Rightarrow f(p_3) \in \{p_2, p_3, p_6\}$

$p_4^3 = e \Rightarrow f^3(p_4) = e \Rightarrow f(p_4) \in \{p_4, p_5\}$

$p_5^3 = e \Rightarrow f^3(p_5) = e \Rightarrow f(p_5) \in \{p_4, p_5\}$

$$P_6^2 = e \Rightarrow f^2(P_6) = e \Rightarrow f(P_6) \in \{P_2, P_3, P_6\}$$

So $|\mathrm{Aut}(S_3)| \leq 2! \times 3! = 12.$

Consider $S_{\{P_2, P_3, P_6\}}$

$$= \left\{ \underset{q_1}{\begin{array}{l} P_2 \to P_2 \\ P_3 \to P_3 \\ P_6 \to P_6 \end{array}},\ \underset{q_2}{\begin{array}{l} P_2 \to P_2 \\ P_3 \to P_6 \\ P_6 \to P_3 \end{array}},\ \underset{q_3}{\begin{array}{l} P_2 \to P_3 \\ P_3 \to P_2 \\ P_6 \to P_6 \end{array}},\ \underset{q_4}{\begin{array}{l} P_2 \to P_3 \\ P_3 \to P_6 \\ P_6 \to P_2 \end{array}},\ \underset{q_5}{\begin{array}{l} P_2 \to P_6 \\ P_3 \to P_2 \\ P_6 \to P_3 \end{array}},\ \underset{q_6}{\begin{array}{l} P_2 \to P_6 \\ P_3 \to P_3 \\ P_6 \to P_2 \end{array}} \right\}$$

q_1 is trivial.

$$\begin{cases} q_2(P_2P_3) = q_2(P_2)\,q_2(P_3) = P_2P_6 = P_5 \\ q_2(P_2P_6) = P_2P_3 = P_4 \end{cases}$$ is consistent with $q_2(P_5) = P_4$, $q_2(P_4) = P_5$.

q_3 and q_6 are also consistent (well-defined), checking similarly.

$$\begin{cases} q_4(P_2P_3) = P_3P_6 = P_4 & q_4(P_2P_6) = P_3P_2 = P_5 & q_4(P_3P_6) = P_6P_2 = P_4 \\ q_4(P_3P_2) = P_6P_3 = P_5 & q_4(P_6P_2) = P_2P_3 = P_4 & q_4(P_6P_3) = P_2P_6 = P_5 \end{cases}$$

q_4 is consistent with $q_4(P_4) = P_4$, $q_4(P_5) = P_5$.

q_5 is consistent, checking similarly.

$$\therefore \mathrm{Aut}(S_3) = \left\{ \begin{array}{l} P_1 \to P_1 \\ P_2 \to P_2 \\ P_3 \to P_3 \\ P_4 \to P_4 \\ P_5 \to P_5 \\ P_6 \to P_6 \end{array},\ \begin{array}{l} P_1 \to P_1 \\ P_2 \to P_2 \\ P_3 \to P_6 \\ P_4 \to P_5 \\ P_5 \to P_4 \\ P_6 \to P_3 \end{array},\ \begin{array}{l} P_1 \to P_1 \\ P_2 \to P_3 \\ P_3 \to P_2 \\ P_4 \to P_5 \\ P_5 \to P_4 \\ P_6 \to P_6 \end{array},\ \begin{array}{l} P_1 \to P_1 \\ P_2 \to P_3 \\ P_3 \to P_6 \\ P_4 \to P_4 \\ P_5 \to P_5 \\ P_6 \to P_2 \end{array},\ \begin{array}{l} P_1 \to P_1 \\ P_2 \to P_6 \\ P_3 \to P_2 \\ P_4 \to P_4 \\ P_5 \to P_5 \\ P_6 \to P_3 \end{array},\ \begin{array}{l} P_1 \to P_1 \\ P_2 \to P_6 \\ P_3 \to P_3 \\ P_4 \to P_5 \\ P_5 \to P_4 \\ P_6 \to P_2 \end{array} \right\}$$

where $P_1 \sim P_6$ are notations in $(*)$. $\square$

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 $\sim = \{(a,b) \in G \times G : b^{-1}a \in H\}$.

2.

Pf. (a). if f is a group homomorphism.

identity. since $f(e) = e$.

$(e.f(e)) = (e.e) = e_{G_f}$. because $(e.e)(x.f(x)) = (x.f(x))$

associativity. $((x.f(x))(y.f(y)))(z.f(z))$

$= (xy.\ f(x)f(y))(z.f(z))$

$= (xy,\ f(xy))(z.f(z))$

$= (xyz.\ f(xyz))$

$= (xyz.\ f(x)f(yz))$

$= (x.f(x))(yz.\ f(yz))$

$= (x\ f(x))((y.f(y))(z.f(z)))$.

inverse. $\forall g_f \in G_f \quad g_f = (g.\ f(g))$

$\Rightarrow g_f^{-1} = (g^{-1}.\ f^{-1}(g))$

Since g^{-1} is unique. $f^{-1}(g)$ is unique.

$g_f \cdot g_f^{-1} = (e.e) = g_f^{-1} \cdot g_f$

since $G_f \subset G \times G$. and $(e,e) \in G_f \neq \phi$

so $f \in \mathrm{Hom}(G,G) \Rightarrow G_f \leq G \times G$

When $G_f \leq G \times G$

$id_{G\times G} = (e,e) \in G_f \Rightarrow f(e) = e$

$(x, f(x)) \in G_f$. $(y, f(y)) \in G_f$. then

$(x, f(x))(y, f(y)) = (xy, f(x)f(y)) \in G_f \Rightarrow f(x)f(y) = f(xy)$

so $G_f \leq G \times G \Rightarrow f \in \mathrm{Hom}(G \times G)$

(b).

Pf. If $H \trianglelefteq G$. s.t. $\sim := \{(a,b) \in G\times G \mid b^{-1}a \in H\}$

$\forall g \in G$. $gHg^{-1} = H$

In this case $G_\sim$ is a group because.

Identity. $(e,e) = id_{G_\sim}$. $(e,e)\cdot(g,h) = (g,h)(e,e) = (g,h)$

Associativity $((x_1, y_1)(x_2, y_2))(x_3, y_3)$, $x_1 \sim y_1$ $x_2 \sim y_2$ $x_3 \sim y_3$

$= (x_1x_2, y_1y_2)(x_3, y_3)$

$= (x_1x_2x_3, y_1y_2y_3)$

$= (x_1, y_1)(x_2x_3, y_2y_3)$

$= (x_1, y_1)((x_2, y_2)(x_3, y_3))$

Inverse. given $(g,h) \in G_\sim$ with $g \sim h$

$(g^{-1}, h^{-1}) \in G_\sim$ because $g^{-1}h \in H \Rightarrow h^{-1}g \in H$

$$(g,h)(g^{-1},h^{-1}) = (g^{-1},h^{-1})(g,h) = (e,e)$$

so $G_\sim$ is a group

since $G_\sim \subset G\times G$. $(e,e)\in G_\sim \neq \phi$. so we have $G_\sim \leq G\times G$.

If $G_\sim \leq G\times G$.

Then $(e,e)\in G_\sim \Rightarrow e\sim e$

$x_1\sim y_1,\ x_2\sim y_2 \Rightarrow x_1x_2 \sim y_1y_2$

$x\sim y \Rightarrow x^{-1}\sim y^{-1}$

let $H=[e] := \{g\in G \mid g\sim e\}$

$H \trianglelefteq G$ because $\forall g\in G.\ \forall h\in H$

$(h,e)\in G_\sim,\ g\sim g \Rightarrow (gh, g)\in G_\sim$

$g^{-1}\sim g^{-1} \Rightarrow (ghg^{-1}, e)\in G_\sim$

$\Rightarrow ghg^{-1}\in H$

At this time $a\sim b$ iff $(a,b)\in G_\sim$

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

iff $b^{-1}a\in H$

i.e. $\sim = \{(a,b)\in G\times G \mid b^{-1}a\in H\}$. □

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 $g\in G$, $S^g = S$.

3. Pf. define function $f_g : S \to S^g$

$$s \mapsto gsg^{-1}$$

Claim f_g is bijection

f_g is obviously a surjection because $S^g = f(S)$

using the cancellation law in group G

$$gs_1g^{-1} = gs_2g^{-1} \Leftrightarrow s_1g^{-1} = s_2g^{-1} \Leftrightarrow s_1 = s_2$$

so f_g is a bijection.

since $S^g \subset S$. if $S \setminus S^g \neq \phi$ suppose $h \in S \setminus S^g$

then $h \in S$. $h \notin f_g(S) \Rightarrow \nexists s \in S$ s.t. $h = gsg^{-1}$

$\Rightarrow \nexists s \in S$ s.t. $(g^{-1})h(g^{-1})^{-1} = s$

$\Rightarrow \nexists s \in S$ s.t. $s = f_{g^{-1}}(h)$

this contradicts with the fact that f_g is a bijection for all $g \in G$.

so $\forall g \in G$. $S \setminus S^g = \phi$ i.e. $S = S^g$. $\square$

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. $H_S = \langle S \rangle$

4. Pf. $H_S \leq G$ because it satisfies the 3 following properties:

① $e \in H_S$

② let $h_1 = s_{11} \cdots s_{1n}$. $h_2 = s_{21} \cdots s_{2n}$

$h_1 h_2 = s_{11} \cdots s_{1n} \cdot s_{21} \cdots s_{2n} \in H_S$

So H_S is closed under group operator

③ let $h = s_1 s_2 \cdots s_n$

then $h^{-1} = s_n^{-1} s_{n-1}^{-1} \cdots s_2^{-1} s_1^{-1}$ $\quad hh^{-1} = h^{-1}h = e$

So H_S is closed under inversion.

If $H \leq G$ and $S \subset H$, and if $\exists h \in H_S$. s.t. $h \notin H$

then $h^{-1} \in H_S \setminus H$

In hw2. Q2(a) I showed that

$$\left.\begin{array}{l} H \leq G \\ H_S \leq G \end{array}\right\} \Rightarrow H \cap H_S \leq G$$

suppose $h = s_1 s_2 \cdots s_n$ where $\forall j. \{s_j, s_j^{-1}\} \cap S \neq \phi$

since $S \subset H \cap H_S \leq G$

so $H \cap H_S$ is closed under inversion and group operation

this contradicts with "$h \notin H_S \cap H$".

So our assumption is false. i.e. $\left.\begin{array}{l} H \leq G \\ S \subset H \end{array}\right\} \Rightarrow H_S \subset H.$ $\square$

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.

5.(a). Pf. Since S is finite. suppose $S=\{r_1\ r_2\ \cdots\ r_n\}$

W.L.O.G suppose $0\notin S$ and $r_k\geqslant 0.\ \forall k$

denote r_k by $\frac{p_k}{q_k}$ where $\gcd(p_k.\ q_k)=1$

let $q=\underset{1\le k\le n}{\operatorname{lcm}} q_k \quad p=\underset{1\le k\le n}{\gcd} p_k$

then $\forall k.\ p\mid p_k.\ q_k\mid q$

Claim. $\forall n_i\in\mathbb{Z}.\ \sum_{i=1}^{n} n_i\cdot r_i \neq \frac{p}{2q}$

$$LHS=\sum_{i=1}^{n}\frac{n_i p_i}{q_i}=\frac{\sum_{i=1}^{n} n_i\left(\frac{q}{q_i}\right)\cdot p_i}{q}$$

since $p\mid p_i.$ we have $p\ \Big|\ \sum_{i=1}^{n} n_i\left(\frac{q}{q_i}\right)p_i$

so $LHS\in\left\{k.\frac{p}{q}\ \Big|\ k\in\mathbb{Z}\right\}\Rightarrow LHS\neq RHS$

so $\exists r\in\mathbb{Q}\setminus\langle S\rangle$ $\square$

(b). Pf Denote the map only switching i and j in $\{1.2.\cdots.n\}$ by (ij)

then $S=\{(12),(23)\cdots(n-1,n)\}$ is a generating set sized. $n-1$

Claim. $f\in S_n\Leftrightarrow\exists s_1 s_2\cdots s_k\in S$ s.t. $f=s_1\circ s_2\circ\cdots\circ s_k$ (allowed to repeat)

$(\Leftarrow)$ is obvious because S_n contains all bijections from $\{1.2.\cdots.n\}$ to itself.

$(\Rightarrow)$ Observe the fact that the sequence $a_1a_2\cdots a_n$ where $a_j\in\{1.2.\cdots.n\}$

can always be sorted to $1\,2\,3 \cdots n$ by switching adjacent elements. The algorithm is called bubble sort. As long as the sequence is finite, this process can easily be reverted. $\square$

(c). Sol. $\sigma = (1.2)$, $\tau = (1\,2 \cdots n)$