Math 534 HW 6

Morgan Gribbins

(1) Prove that every element in S_n for $n > 1$ can be written as a product of transpositions of the form $(1\ k)$.

Proof by induction that $(i\ i+1)$ can be written as a product of transpositions of the form $(1\ k)$. First, we will prove the case of $i = 2$. This is the transposition $(2\ 3)$, which is equivalent to $(12)(13)(12)$, so this case may be written as a product of transpositions of the form $(1\ k)$.

Now, we will assume that $(j\ j+1)$ can be written in this form, and show that this implies $(j+1\ j+2)$ can be written in this form. The permutation $(1\ j+1)(1\ j+2)(1\ j+1)(j\ j+1) = (j+1\ j+2)$, so it is evident that this property holding for j implies it holds for $j+1$, so this is possible for every element in S_n.

(2) Prove that the 4-cycle $(1234) \in S_n$ cannot be written as a product of 3-cycles.

The 4-cycle (1234) is equivalent to $(14)(13)(12)$ and as such is odd. Any 3-cycle (abc) can be written as $(ac)(ab)$, so it is even. Therefore, any product of 3-cycles must be even. This means that any product of 3-cycles has a different parity than (1234), so these permutations can not be equal.

(3) Show that a permutation of odd order must be an even permutation. Is every permutation of even order an odd permutation?

Consider an arbitrary permutation of order $2n+1$, which can be written as $(a_1 a_2 ... a_{2n+1}$. This permutation can be written as $(a_{2n+1} a_1)(a_{2n} a_1)...(a_2 a_1)$, which has $2n$ terms, and as such is even. Therefore, an odd ordered permutation must be even.

This is not true. Consider the permutation $(34)(12)$. This has even order (2) and is an odd permutation.

(4) Prove that the groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, \cdot)$ are not isomorphic.

Assume that there is some isomorphism between these two groups, $\phi : (\mathbb{Z}, +) \to (\mathbb{Q}, \cdot)$. As this is a isomorphism, we have $\phi(a+b) = \phi(a) \cdot \phi(b)$. Therefore, we have $\phi(2) = \phi(1+1) = \phi(1) \cdot \phi(1)$ and $\phi(3) = \phi(1+1+1) = \phi(1) \cdot \phi(1) \cdot \phi(1)$. This means there is some element a in $\mathbb{Q}$ such that $a^2 = a^3$ (with regular rules of multiplication, and with 0 not in this group), so

$a = 1$. However, we have $\phi(0) = 1$, so this contradicts the 1-1 property of an isomorphism. Therefore, this must not be an isomorphism, and these two groups cannot be isomorphic.

(5) Let $\phi : G_1 \to G_2$ be a homomorphism.

(5a) Define the *image* of G_1 under ϕ to be

$$\phi(G_1) = \{g \in G_2 : \exists a \in G_2, \ g = \phi(a)\}$$

Prove that this is a subgroup of G_2.

In order for $\phi(G_1)$ to be a subgroup of G_2, it must be closed, it must contain the identity, and it must contain inverses.

Proof that $\phi(G_1)$ is closed. Let $g_1, g_2 \in \phi(G_1)$. Due to the definition of the image of G_1, we have $\exists a_1, a_2$ such that $\phi(a_1) = g_1$ and $\phi(a_2) = g_2$. By definition of a homomorphism, we have $\phi(a_1 a_2) = \phi(a_1)\phi(a_2) = g_1 g_2$, so $a_1 a_2 \in G_1$ satisfies $\phi(a_1 a_2) = g_1 g_2$, so $g_1, g_2 \in \phi(G_1) \implies g_1 g_2 \in \phi(G_1)$.

Proof that $\phi(G_1)$ contains the identity. Let e be the identity in G_1 and i be the identity in G_2. As $e \in G_1$, $\phi(e) = \phi(ee) = \phi(e)\phi(e) \in G_2$ (and $\phi(e) \in \phi(G_1)$). Therefore, we have $\phi(e) = \phi(e)\phi(e) \implies i\phi(e) = \phi(e)\phi(e) \implies i = \phi(e)$, and $\phi(e) \in \phi(G_1)$, so $\phi(G_1)$ contains the identity.

Proof that $\phi(G_1)$ contains inverses. Let $a \in G_1$. This implies that $a^{-1} \in G_1$, so we have $\phi(a)$ and $\phi(a^{-1}$ in $\phi(G_1)$. Also, $\phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) \implies \phi(e) = \phi(a)\phi(a^1)$ where $\phi(e)$ is the identity of $\phi(G_1)$, so $\phi(a) \in \phi(G_1) \implies \phi(a^{-1}) = \phi(a)^{-1} \in \phi(G_1)$, so this group has inverses.

Therefore, $\phi(G_1)$ is a subgroup of G_2.

(5b) Define the *kernel* of ϕ to be

$$\ker \phi = \{a \in G_1 : \phi(a) = e\}$$

where $e \in G_2$ is the identity. Prove that this is a subgroup of G_1.

In order for $\ker \phi$ to be a subgroup of G_1, it must be closed, it must contain the identity, and it must contain inverses.

Proof that $\ker \phi$ is closed. Let $a, b \in \ker \phi$. By definition of $\ker \phi$, we have $\phi(a) = e$ and $\phi(b) = e$. Consider the element $ab \in G_1$. $\phi(ab) = \phi(a)\phi(b) = ee = e$, so $ab \in \ker \phi$. Therefore, $\ker \phi$ is closed.

Proof that $\ker \phi$ contains the identity. Let e_1 be the identity of G_1 and e_2 be the identity of G_2. $e_1 \in \ker \phi$ if $\phi(e_1) = e_2$. We have $\phi(e_1) = \phi(e_1 e_1 = \phi(e_1)\phi(e_1) \implies e_2\phi(e_1) = $

$\phi(e_1)\phi(e_1) \implies e_2 = \phi(e_2)$, so the identity (of G_1) is in $\ker \phi$).

Proof that $\ker \phi$ contains inverses. Let $a \in \ker \phi$. This means that $\phi(a) = e$ and $\phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = e \implies e\phi(a^{-1}) = e \implies \phi(a^{-1}) = e$, (the e-s in this equation being the identity of G_2) so $a \in \ker \phi \implies a^{-1} \in \ker \phi$.

Therefore, $\ker \phi$ is a subgroup of G_1.

(6) Is the function $\psi : \mathbb{Z}/12 \to \mathbb{Z}/10$ defined by $\psi(k) = 3k$ a homomophism? If so, prove it, and if not, explain why not.

This is a homomorphism. Let $a, b \in \mathbb{Z}/12$. Let us examine $\phi(a + b)$. This is equal to $3(a + b) \mod 10 = 3a + 3b \mod 10$. Considering $\phi(a) + \phi(b) = 3a + 3b \mod 10$, it is clear that these quantities are equal. Therefore, this is a homomorphism.