Problem Set 1

Daniel Halmrast

October 17, 2017

Problem 1

Show that the cycle $(1, 2, \ldots, n)$ can be written as a product of $n-1$ transpositions, but no fewer.

Proof. Trivially, this holds for $n = 2$. So assume $n \geq 3$.

First, note that the decomposition

$$(1, 2, \ldots, n) = (1, n)(1, n-1), \ldots, (1, 3)(1, 2)$$

is a product of $n-1$ transpositions as desired.

Now, consider an arbitrary decomposition of the cycle

$$(1, 2, \ldots, n) = \tau_1 \tau_2 \ldots \tau_m$$

where each τ_i is a transposition. Observe that for any decomposition, each number from 1 to n must appear in at least 1 transposition, since the permutation admits no fixed points.

Next, let's count how many unique numbers appear in the decomposition. τ_1 will introduce two unique numbers, leaving $n-2$ left to appear. Since the permutation has no disjoint subcycles, there must exist some τ_{i_1} that is not disjoint to τ_1. At most, τ_{i_1} will introduce one new unique number (since one is shared by τ_1, leaving at least $n-3$ numbers to be introduced by $m-2$ traspositions.) Similarly, there must be some τ_{i_2} that shares a number with either τ_1 or τ_{i_1}, and will introduce at most one new number.

Following this process shows that each τ_{i_k} will introduce at most one new number to the decomposition, so to introduce $n-2$ numbers requires at least $n-2$ transpositions.

Considering also τ_1, we see that there must be at least $n-1$ total transpositions in the decomposition.

□

Problem 2

Let $G \leq S_n$, with $G \not\subset A_n$. Show that exactly half of the permutations in G are even.

Proof. We know that $e \in G$ and there is some $\sigma \in S_n \setminus A_n$ such that $\sigma \in G$.

Now, consider the cyclic subgroup $\langle \sigma \rangle$ generated by this element. Since G is finite, this subgroup has finite order, call it m. I assert that m must be even, since if m were odd, it would imply that σ^m, which is an odd permutation, is equal to e. But since e is an even permutation, such a relation cannot exist. Thus, m must be even.

Furthermore, for each m, the parity of m determines the parity of σ^m. This is made clear by considering a decomposition of $\sigma = \tau_1 \dots \tau_k$ for some odd k. Then, $\sigma^m = \prod_m \tau_1 \dots \tau_k$ before reduction has $m * k$ transpositions. When reducing this word, if two adjacent transpositions are inverses, both are removed. Thus, the reduced word has an even number of symbols less than $m * k$. Since $m * k$ is even, the reduced word is also even as desired.

Thus, the cyclic group $\langle \sigma \rangle$ has exactly half of its permutations as even permutations.

Observe that, for each coset $\omega\langle \sigma \rangle$ of $\langle \sigma \rangle$, either ω is even, or it is odd. If ω is even, it will not change the parity of any permutation, and the coset $\omega\langle \sigma \rangle$ has exactly half of its permutations as even permutations. If ω is odd, on the other hand, it will flip the parity of each permutation, but $\omega\langle \sigma \rangle$ will still have exactly half of its permutations as even permutations.

Since G is partitioned by cosets of the subgroup $\langle \sigma \rangle$, it can be written as a union of the disjoint cosets. Each coset has exactly half of its elements as even permutations, so the whole group G has the same property. □

PROBLEM 3

Show that a permutation is regular if and only if it is a power of a permutation with no fixed points.

Proof. (=>) Let $\sigma \in S_n$ be such that it can be written as a product of disjoint cycles $\omega_1 \dots \omega_m$ of the same length. Now, since each number from 1 to n will appear exactly

once in the decomposition, the order of any ω_i is just $l = \frac{n}{m}$. So, let

$$\begin{aligned}\omega_1 &= (k_{1_1} k_{1_2} \dots k_{1_l}) \\ \omega_2 &= (k_{2_1} k_{2_2} \dots k_{2_l}) \\ &\vdots \\ \omega_m &= (k_{m_1} k_{m_2} \dots k_{m_l})\end{aligned}$$

Then, it is easy to verify that

$$\sigma = (k_{1_1} k_{2_1} \dots k_{m_1} k_{1_2} \dots k_{m_l})^m$$

as desired.

(<=) For the other direction, assume (without loss of generality) $\sigma = (12 \dots n)^m$ for some $0 < m < n$, which implies that the order of σ is the smallest number l such that $lm = 0 \pmod{n}$. Now, if m is relatively prime to n, then the order of σ is n, and can be written as the single permutation

$$\sigma = (1 \ m \ 2m \dots (n-1)m)$$

where multiplication is taken modulo n.

Next, consider the case where m divides n, so that the order of σ is $l = \frac{n}{m}$. Then, each number $1 \leq i \leq l - 1$ moves in a disjoint subcycle,

$$\omega_i = (i \ i + m \ i + 2m \dots i + (l-1)m)$$

and thus $\sigma = \prod_i \omega_i$ as desired. □

Problem 4

Show that a permutation group is regular if and only if each permutation moves all points or no points.

Proof. (=>) Note that regular permutations are characterized by being powers of a cycle that moves all points. So, if a group is made up of regular permutations, it must be made up of powers of cycles that move all points. Now, since a power of a cycle also moves all points (unless it is equal to the identity, in which case it moves no points), each element of a regular group moves all points, or moves no points.

(<=) Now, let $G \subset S_n$ be a permutation group such that each element of G either moves all points or moves no points. If $g \in G$ moves no points, then g is the identity, which is regular.

So, let $g \in G$ be an element that moves all points. For a contradiction, assume that g has a disjoint cycle decomposition with two elements σ, ω of differing order. Let $|\sigma| = j$ and $|\omega| = k$. Without loss of generality, let $j < k$. Then, the element g^j fixes all points in the σ subcycle, but does not fix all points in the ω subcycle (since the order of ω is

not j). This violates the assumption that all the elements of G either fix all points or move all points, since $g^j \in G$.

Therefore, every element of G moves all points, or moves no points as desired.

□

Problem 5

Show that in any group, ab and ba have the same order.

Proof. Suppose first that the order of ab is finite. Then, for some n, $(ab)^n = e$. Now, take the conjugate with a to obtain

$$a^{-1}(ab)^n a = a^{-1}ea = e$$
$$(ba)^n = e$$

Thus, the order of ba divides the order of ab, since $(ba)^n = e$. However, reversing the roles of a and b shows that the order of ab divides the order of ba. Thus, since they both divide each other, they must be equal.

Suppose instead that the order of ab is infinite, and for a contradiction assume that ba had finite order. Then, by the above argument, the order of ab must equal the order of ba, which is a contradiction.

Thus, the order of ab is equal to the order of ba. □

Problem 6

Let G be any group, and $n > 2$. Show that there are an even number of elements order n in G.

Proof. Consider the set E_n of all elements of order $n > 2$ in G, along with the equivalence relation $g \sim g^{-1}$. Since $n > 2$, it is known that $g^{-1} \neq g$. Furthermore, since $(g^{-1})^{-1} = g$, each equivalence class has exactly two elements.

Thus, since E_n is partitioned by $\sim$ into disjoint sets, each with two elements, the size of E_n must be a multiple of two. Hence, it must be even. □

Problem 7

Show that any group of even order has an element of order 2.

Proof. To prove this, we start by proving the case for Abelian groups, and we will induct on the order of the group.

The base case of $|G| = 2$ is trivial.

Now, let G be an Abelian group of even order, and let $g \in G$. If $|g|$ is even, then the element $g^{\frac{|g|}{2}}$ has order 2, and the proof is complete. So, suppose $|g|$ is odd. Then, consider the quotient $G/\langle g \rangle$. Since $|G|$ is even and $|\langle g \rangle|$ is odd, Lagrange's theorem tells us that $|G/\langle g \rangle|$ is even, and has smaller order than G. By the inductive hypothesis, we are done.

Now, consider a more general group G. By the class equation, we have

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

For $Z(G)$ the center of G, $C_G(x_i)$ the centralizer of x_i, and the sum ranging over representatives of the different conjugacy classes in G not in the center.

Now, if $|Z(G)|$ is even, then it contains an element of order 2. This is clear, since the center is Abelian, and by the previous result any Abelian group of even order has an element of order 2.

Suppose, then, that $|Z(G)|$ is odd. Then, there must be at least one element $[G : C_G(x_j)]$ of the sum which is also odd. However, by Lagrange's theorem, this means that $|C_G(x_j)|$, which is a proper subgroup of G, has even order. Thus, by the inductive hypothesis, it contains an element of order 2.

Therefore by induction, any group of even order has an element of order 2. □

Problem 8

Show that every finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic.

Proof. Let S be a finite subset of $\mathbb{Q}$. In particular, the elements of S have a least common denominator d, so that for each $s_i \in S$, $s_i = k_i * \frac{1}{d}$ for some integer k_i. Thus, $s_i \in \langle \frac{1}{d} \rangle$. Since each s_i is in the subgroup $\langle \frac{1}{d} \rangle$, by the definition of a generated group,

$$\langle S \rangle \leq \langle \frac{1}{d} \rangle$$

Subgroups of cyclic groups are cyclic, so the subgroup $\langle S \rangle$ is cyclic. □