James Lee Crowder

Math 430
Dr. Songhao Li
Spring 2016

HOMEWORK 3 SOLUTIONS
Due 2/15/16

Part II Section 9 Exercises

4. Find the orbits of $\sigma : \mathbb{Z} \to \mathbb{Z}$ defined by $\sigma(n) = n + 1$.

Solution: We show that the only orbit is $\mathbb{Z}$. Let $i, j \in \mathbb{Z}$. Then $j - i \in \mathbb{Z}$ and $\sigma^{j-i}(i) = i + (j - i) = j$, and thus σ has only one orbit.

■

5. Find the orbits of $\sigma : \mathbb{Z} \to \mathbb{Z}$ defined by $\sigma(n) = n + 2$.

Solution: We will show that the orbits of σ are $2\mathbb{Z}$ and $2\mathbb{Z} + 1$, the even and odd integers respectively. Let $2i, 2j \in 2\mathbb{Z}$. Then $2j - 2i = 2(j - i) \in 2\mathbb{Z}$, and thus $\sigma^{j-i}(2i) = 2i + 2(j - i) = 2j$. Similarly, suppose $2p+1, 2q+1 \in 2\mathbb{Z}+1$. Then $(2q+1)-(2p+1) = 2(q-p) \in 2\mathbb{Z}$, and so $\sigma^{q-p}(2p+1) = 2p+1+2(q-p) = 2q+1$. Thus, $2\mathbb{Z}$ and $2\mathbb{Z} + 1$ are the orbits of σ.

■

6. Find the orbits of $\sigma : \mathbb{Z} \to \mathbb{Z}$ defined by $\sigma(n) = n - 3$.

Solution: Similarly to the prior two problems, the orbits of σ are $3\mathbb{Z}, 3\mathbb{Z} + 1$, and $3\mathbb{Z} + 2$.

■

9. Compute the following product of permutations in S_8: $(1\,2)(4\,7\,8)(2\,1)(7\,2\,8\,1\,5)$.

Solution: Since $(7\,2\,8\,1\,5)$ maps 1 to 5, $(2\,1)$ fixes 5, $(4\,7\,8)$ fixes 5, and $(1\,2)$ fixes 5, $(1\,2)(4\,7\,8)(2\,1)(7\,2\,8\,1\,5)$ maps 1 to 5. Similarly, we compute $(1\,2)(4\,7\,8)(2\,1)(7\,2\,8\,1\,5) = (1\,5\,8)(2\,4\,7)$.

■

12. Express $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$ as a product of disjoint cycles and as a product of transpositions.

Solution: Since $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix} = (1\,3\,4\,7\,8\,6\,5\,2)$ is a cycle, we directly compute that

$$(1\,3\,4\,7\,8\,6\,5\,2) = (1\,2)(1\,5)(1\,6)(1\,8)(1\,7)(1\,4)(1\,3)$$

■

16. Find the maximum possible value for an element of S_7.

Proof. We first show general result that will be useful in its own right: if $\prod_{I=1}^{N} \gamma_I$ is a product of disjoint cycles of length ℓ_I, then $\left|\prod_{I=1}^{N} \gamma_I\right| = \text{lcm}(\ell_1, \ldots, \ell_N)$. Let $l = \text{lcm}(\ell_1, \ldots, \ell_N)$. Then $l = \ell_I d_I$ for some $d_I \in \mathbb{N}$. Then, since disjoint cycles commute, $\left(\prod_{I=1}^{N} \gamma_I\right)^l = \prod_{I=1}^{N} \gamma_I^l = \prod_{I=1}^{N} (\gamma_I^{\ell_I})_I^d = \prod_{I=1}^{N} \iota^{d_I} = \iota$. Suppose $n < l$. Then n is not a common multiple of $\ell_1, \ldots, \ell_N$. Without loss of generality, suppose n is not a multiple of ℓ_1. Then, by the Division Algorithm, $n = q\ell_1 + r$ for some $q, r \in \mathbb{Z}$ with $0 < r < \ell_i$. Let $i \in \gamma_1$. Then $i \notin \gamma_I$ for $I \neq 1$ since the γ_I are disjoint, and thus

$$\left(\prod_{I=1}^{N} \gamma_I\right)^n (i) = \gamma_1^n(i) = \gamma_1^{q\ell_1 + r}(i) = (\gamma_1^{\ell_1})^q \circ \gamma_1^r(i) = \iota^q \circ \gamma_1^r(i) = \gamma_1^r(i)$$

Since γ_1 is a cycle and $0 < r < \ell_1$, $\gamma_1(i) \neq i$; in particular, $\left(\prod_{I=1}^{N} \gamma_I\right)^n \neq \iota$. Thus, $\left|\prod_{I=1}^{N} \gamma_I\right| = \text{lcm}(\ell_1, \ldots, \ell_N)$.

Now, by Theorem 9.8, we can always write a given $\sigma \in S_n$ as a product of disjoint cycles $\prod_{I=1}^{N} \gamma_I$. Since $\sigma \in S_n$, we must have $\sum_{I=1}^{N} \ell_I \leq n$ if the γ_I are disjoint cycles (we only have n letters to permute, and cannot permute them multiples times). Since every natural number is a multiple of 1, we may assume that $\sum_{I=1}^{N} \ell_I = n$ without changing the value of $\text{lcm}(\ell_1, \ldots, \ell_N)$ (perhaps by thinking of the fixed elements as "1-cycles"). Thus, finding an element of maximal order in S_n amounts to finding a partition of n (an unordered list of natural numbers $n_1, \ldots, n_M$ such that $\sum_{J=1}^{M} n_J = n$) with maximal least common multiple of the members of the partition. Then any product of cycles of these lengths will have maximal order. For example, in S_7, we need a list of natural numbers $\{n_1, \ldots, n_m\}$ such that $\sum_{i=1}^{m} n_i = 7$ and $\text{lcm}(n_1, \ldots, n_m)$ is as high as possible.

Here, we write each partition of 7 along with the least common multiple of its members:

$$1+1+1+1+1+1+1=7;\quad \mathrm{lcm}(1,1,1,1,1,1,1)=1$$
$$2+1+1+1+1+1=7;\quad \mathrm{lcm}(2,1,1,1,1,1)=2$$
$$2+2+1+1+1=7;\quad \mathrm{lcm}(2,2,1,1,1)=2$$
$$2+2+2+1=7;\quad \mathrm{lcm}(2,2,2,1)=2$$
$$3+1+1+1+1=7;\quad \mathrm{lcm}(3,1,1,1,1)=3$$
$$3+2+1+1=7;\quad \mathrm{lcm}(3,2,1,1)=6$$
$$3+2+2=7;\quad \mathrm{lcm}(3,2,2)=6$$
$$4+1+1+1=7;\quad \mathrm{lcm}(4,1,1,1)=4$$
$$4+2+1=7;\quad \mathrm{lcm}(4,2,1)=4$$
$$4+3=7;\quad \mathrm{lcm}(4,3)=12$$
$$5+1+1=7;\quad \mathrm{lcm}(5,1,1)=5$$
$$5+2=7;\quad \mathrm{lcm}(5,2)=10$$
$$6+1=7;\quad \mathrm{lcm}(6,1)=6$$
$$7=7;\quad \mathrm{lcm}(7)=7$$

Thus, any product of two disjoint cycles, one of length 4 and one of length 3 (say, $(1\,2\,3\,4)(5\,6\,7)$) will produce an element of order $\mathrm{lcm}(4,3)=12$, and this is the maximal possible order for an element of S_7. In general, it is not easy to determine this maximal number, as the number of partitions of n grows quickly as n gets larger. The function that associates this maximal number to n is known as Landau's function. ■

27. Suppose $n \in \mathbb{N}$ such that $n \geq 3$. Show that every $\sigma \in S_n$ can be written as a product of at most $n-1$ transpositions. If σ is not a cycle, show that σ can be written as a product of at most $n-2$ transpositions.

Thank you to Justin Finkel and Renee Mirka for correcting a bounding error I did not catch on my initial attempted proof for this problem.

Proof. Suppose $\sigma \in S_n$. If $\sigma = \iota$, then $\sigma = (1\,2)(1\,2)$ is the desired product. Otherwise, by Theorem 9.8 we can write $\sigma = \prod_{i=1}^{m} \gamma_i$, where the γ_i are disjoint cycles and $m \in \mathbb{N}$. Note that, since the cycles γ_i are disjoint, the sum of the lengths ℓ_i of the cycles γ_i must be at most n, and so $\sum_{i=1}^{m} \ell_i \leq n$ (in short, none of the numbers $1, 2, \ldots, n$ is written more than once in the cycle decomposition). If γ_i is of length ℓ_i, then $\gamma_i = \prod_{j_i=1}^{\ell_i - 1} \tau_{j_i}$, where each τ_{j_i} is a transposition, as in Definition 9.11. Thus, $\sigma = \prod_{i=1}^{m} \gamma_i = \prod_{i=1}^{m} \left[\prod_{j_i=1}^{\ell_i-1} \tau_{j_i} \right]$ gives σ as a product of $\sum_{i=1}^{m} (\ell_i - 1) = \left(\sum_{i=1}^{m} \ell_i \right) - m \leq n - m \leq n-1$ transpositions.

As above, if σ is not a cycle, then $m \geq 2$, and thus we have written σ as a product of $\sum_{i=1}^{m} (\ell_i - 1) = \left(\sum_{i=1}^{m} \ell_i \right) - m \leq n - m \leq n-2$ transpositions. In fact, if σ is a cycle of length $m \leq n-1$, then we can write σ as a product of at most $m - 1 \leq n-2$ transpositions as in Definition 9.11, i.e. only cycles of length n require $n-1$ transpositions. ∎

29. Show that for every subgroup H of S_n with $n \geq 2$, either all the permutations of H are even or exactly half of them are even.

Proof. Suppose H contains an odd permutation, say $\omega = \prod_{i=1}^{2m+1} \tau_i$ for $m \in \mathbb{N}$ and some transpositions τ_i. Set $H_e = H \cap A_n$ and $H_o = H \setminus H_e$. Define the function $\mathbf{S} : H_e \to H_o$ by $\mathbf{S}(\epsilon) = \omega \circ \epsilon$. If $\epsilon \in H_e$, then ϵ is even, and hence $\lambda \circ \epsilon$ is odd, and so $\mathbf{S}$ does in fact map H_e into H_o. We will now show that $\mathbf{S}$ is a bijection, which will yield the result. Suppose $\mathbf{S}(\epsilon) = \mathbf{S}(\varepsilon)$. Then, $\omega \circ \epsilon = \omega \circ \varepsilon$, and thus $\epsilon = \varepsilon$ by cancellation. Thus, $\mathbf{S}$ is injective. Let $\sigma \in H_o$. The, since σ is odd and ω is odd, $\omega^{-1} \circ \sigma$ is even, and hence in H_e since $\omega, \sigma \in H$. Then $\mathbf{S}(\omega^{-1} \circ \sigma) = \omega \circ (\omega^{-1} \circ \sigma) = (\omega \circ \omega^{-1}) \circ \sigma = \iota \circ \sigma = \sigma$, and so $\mathbf{S}$ is surjective. Then $\mathbf{S}$ is a bijection, and therefore $|H_e| = |H_o|$, i.e. H has exactly as many even permutations as odd permutations.

Therefore, either all permutations in H are even or exactly half of them are even. ∎

32. Let A be an infinite set, and K the set of all $\sigma \in S_A$ such that $\big|\{a \in A \mid \sigma(a) \neq a\}\big| \leq 50$. Is K a subgroup of S_A?

Solution: We will show that K is not a subgroup of S_A. Let $a_1, \ldots, a_{100} \in A$. Then $(a_1\, a_2\, \ldots\, a_{50})$ and $(a_{51}\, a_{52}\, \ldots\, a_{100})$ are in K, but their product $(a_1\, a_2\, \ldots\, a_{50})(a_{51}\, a_{52}\, \ldots\, a_{100})$ is not since $(a_1\, a_2\, \ldots\, a_{50})(a_{51}\, a_{52}\, \ldots\, a_{100})$ moves $100 > 50$ elements.

■

34. Show that if σ is a cycle of odd length, then σ^2 is a cycle.

Proof. Let $n \geq 3$ (so that there are odd cycles in S_n), and suppose $\sigma = (a_1\, a_2\, \cdots\, a_{2m+1})$ for some $m \in \mathbb{N}$ and distinct $a_i \in \{1, 2, \ldots, n\}$. Then $\sigma^2 = (a_1\, a_3\, \cdots\, a_{2m-1} \;\; a_{2m+1} \;\; a_2\, a_4\, \cdots\, a_{2m-2} \;\; a_{2m})$ is a cycle. ■

39. Show that $S_n = \big\langle (1\,2), (1\,2\, \cdots\, n-1 \;\; n) \big\rangle$.

Proof. By Corollary 9.12, it suffices to show that for each transpositions $(i\,j) \in S_n$, $(i\,j) \in \big\langle (1\,2), (1\,2\, \cdots\, n-1 \;\; n) \big\rangle$. Towards this, we note that for $1 \leq i < j \leq n$, $(i\,j) = (i \;\; i+1)(i+1 \;\; i+2) \cdots (j-2 \;\; j-1)(j-1 \;\; j)(j-2 \;\; j-1) \cdots (i+1 \;\; i+2)(i \;\; i+1)$. Thus, to generate the transpositions, it is enough to generate the transpositions of the form $(k \;\; k+1)$ for $1 \leq k \leq n-1$. Noting that $(1\,2\, \cdots n)^{k-1}(2) = k+1$ and $(1\,2\, \cdots\, n)^{n-k+1}(k) = 1$, we have

$$(1\,2\, \cdots n)^{k-1}(1\,2)(1\,2\, \cdots n)^{n-k+1}(k) = k+1$$

Similarly, since $(1\,2\, \cdots n)^{k-1}(1) = k$ and $(1\,2\, \cdots\, n)^{n-k+1}(k+1) = 2$, we have

$$(1\,2\, \cdots n)^{k-1}(1\,2)(1\,2\, \cdots n)^{n-k+1}(k+1) = k$$

For all other $l \neq k$, $(1\,2\, \cdots n)^{n-k+1}(l) \neq 1, 2$, and so $(1\,2)$ fixes $(1\,2\, \cdots n)^{n-k+1}(l)$. Then

$$(1\,2\, \cdots n)^{k-1}(1\,2)(1\,2\, \cdots n)^{n-k+1}(l) = (1\,2\, \cdots n)^{k-1}\Big((1\,2\, \cdots n)^{n-k+1}(l)\Big) = (1\,2\, \cdots n)^{n}(l) = \iota(l) = l$$

and so $(1\,2\, \cdots n)^{k-1}(1\,2)(1\,2\, \cdots n)^{n-k+1} = (k \;\; k+1)$. Thus, every $(k \;\; k+1) \in \langle (1\,2), (1\,2\, \cdots\, n) \rangle$. Then every $(i\,j) \in \langle (1\,2), (1\,2\, \cdots\, n) \rangle$, and hence $S_n = \langle (1\,2), (1\,2\, \cdots\, n) \rangle$ by Corollary 9.12. ■