MATH 351 – Modern Algebra I
Selected Solutions for Problem Set 9
November 30, 2018

6.26. By Theorem 6.6 in Lee, we know that every $\sigma \in S_n$ is a product of transpositions, but those transpositions can contain any of the (ab), with $1 \le a < b \le n$. On the other hand, by Lemma 6.2, we know that

$$(1a)(1b)(1a) = (1a)(1b)(1a)^{-1} = (ab).$$

Hence in any factorization of σ into transpositions, we can replace any transposition (ab) with $a, b \ne 1$ by the product $(1a)(1b)(1a)$ as above. This shows that every $\sigma \in S_n$ can be written as a product of the "special" transpositions $(1i)$ with $2 \le i \le n$.

6.28. There are many different proofs of this fact. Let's look at two, both of which are based on Exercise 6.26 above.

Proof 1: (This one might be the "slickest".) Letting $\sigma = (12)$ and $\tau = (12\cdots n)$ as in the problem statement, note that Lemma 6.2 implies:

$$\begin{aligned} \tau\sigma\tau^{-1} &= (23) \\ \tau(23)\tau^{-1} &= \tau^2\sigma\tau^{-2} = (34) \\ \tau(34)\tau^{-1} &= \tau^3\sigma\tau^{-3} = (45), \end{aligned}$$

and hence, continuing in the same way every *"consecutive"* transposition $(k\ k+1)$ with $1 \le k \le n-1$ can be written as required by the problem. Then, using Lemma 6.2 again, note that

$$\begin{aligned} (23)(12)(23) &= (13) = (\tau\sigma\tau^{-1})\sigma(\tau\sigma\tau^{-1}) \\ (34)(13)(34) &= (14) = (\tau^2\sigma\tau^{-2})(\tau\sigma\tau^{-1})\sigma(\tau\sigma\tau^{-1})(\tau^2\sigma\tau^{-2}) \end{aligned}$$

and similarly, all of the "special transpositions" $(1i)$ from Exercise 6.26 can be written as products of powers of σ and τ. It follows from Exercise 6.26, then, that every $\rho \in S_n$ can be written in this way too.

Proof 2a: A second way to derive the same conclusion (using Exercise 6.26 in a similar way), is to alternate conjugating 2-cycles and n-cycles, like the following: We have, by Lemma 6.2,

$$\begin{aligned} \sigma\tau\sigma^{-1} &= (2134\cdots n) = \tau_2 \\ \tau_2\sigma\tau_2^{-1} &= (31) = (13) \\ (13)\tau_2(13) &= (2314\cdots n) = \tau_3 \\ \tau_3(13)\tau_3^{-1} &= (41) = (14) \end{aligned}$$

and continuing in the same way, we get all the $(1i)$ with $2 \le i \le n$ as products of powers of σ and τ.

Proof 2b: Proof 2a can also be phrased as an argument *by induction* as follows. We want to show that in S_n, all of the "special" transpositions $(1i)$ for $2 \le i \le n$ can be obtained as products of powers of σ and τ. The base case is $i = 2$ and there is nothing to prove since $\sigma = (12)$. So now let's assume that we have shown $(12), (13), \ldots, (1k)$ can be written this way. Consider $(1\ k+1)$. Then, following what we did in Proof 2a, we consider the product giving the element we called τ_k above:

$$\tau_k = (1k)(1\ k-1)\cdots(13)(12)\tau(12)(13)\cdots(1\ k-1)(1k)$$

By Lemma 6.2, since the product on the right of τ is the inverse of the product on the left of τ, this equals

$$\tau_k = (2\ 3\ 4\ \cdots\ k\ 1\ k+1\ k+2\ \cdots\ n).$$

(In the n-cycle τ, we're transposing the 1 and the 2, then the 1 and the 3, etc. up to the 1 and the k, so $2, 3, \ldots, k$ all end up to the left of 1, and the remaining numbers $k+1, \ldots, n$ have not moved.) By Lemma 6.2 yet again, then

$$\tau_k(1k)\tau_k^{-1} = (k+1\ 1) = (1\ k+1)$$

is a product of powers of τ and σ, since τ_k and $(1k)$ are such products (that's the induction hypothesis) and this finishes the proof.

7.8. We want to show that if a is odd order, then $C(a) = C(a^4)$. We'll set this up as a proof showing each of these sets is contained in the other.

$\subseteq$: Let $g \in C(a)$. Then $ga = ag$, so

$$ga^4 = (ga)a^3 = (ag)a^3 = a(ga)a^2 = a(ag)a^2 = a^2(ga)a = a^3ga = a^4g.$$

Hence $g \in C(a^4)$, so $C(a) \subseteq C(a^4)$. (Note: We don't need the hypothesis that a has odd order for this inclusion.)

$\supseteq$: Now let $g \in C(a^4)$. By definition this means $ga^4 = a^4g$. We have to show this implies $ga = ag$ when $|a|$ is odd. Let $k = |a|$. Then by integer division we have $k = 4q + r$ with $0 \le r < 4$. But note $r = 0, 2$ are not possible, since then k would be even. This says there are two possible values for r, namely $r = 1$ and $r = 3$. We handle each of those cases separately.

If $r = 1$, then $a^{4q+1} = e$, so $a = a^{-4q}$. Note that $a^{-4q} = (a^4)^{-q}$. Since we have $ga^4 = a^4g$, we also have $a^{-4}g = ga^{-4}$ by multiplying both sides of the previous equation by a^{-4} on the left and the right. It follows that $ga^{-4q} = a^{-4q}g$ for all integers q. Hence

$$ga = ga^{-4q} = a^{-4q}g = ag$$

and $g \in C(a)$. This shows $C(a^4) \subseteq C(a)$ when $|a| = 4q + 1$.

If $r = 3$, then $a^{4q+3} = e$, so $a = a^{4(q+1)}$. Note that $a^{4(q+1)} = (a^4)^{q+1}$. If $g \in C(a^4)$, then it follows that $ga^{4(q+1)} = a^{4(q+1)}g$. Hence

$$ga = ga^{4(q+1)} = a^{4(q+1)}g = ag$$

and $g \in C(a)$. This shows $C(a^4) \subseteq C(a)$ when $|a| = 4q + 3$ as well.