HW 3 Selected Solutions

Prof. Shahed Sharif

2.26 Let me prove the following claim first:

Claim. *Suppose* $\beta = (a_0\, a_1\, \cdots\, a_{n-1})$. *Suppose* $n = rt$ *for positive integers* r, t. *Then*

$$\beta^t = (a_0\, a_t\, \ldots\, a_{n-t})(a_1\, a_{t+1}\, \ldots\, a_{n-t+1}) \cdots (a_{r-1}\, \ldots\, a_{n-1}). \tag{1}$$

In particular, β^t *is a product of* t *disjoint* r*-cycles.*

Proof. Since $n = rt$, one sees that each factor is an r-cycle. The fact that there are t disjoint cycles follows easily. So we just have to show that the equality holds.

From the hint in 2.22, we have that $\beta^k(a_0) = a_k$ for $0 \le k \le n-1$. In particular, $\beta^t(a_0) = a_t$. But then $0 \le i \le n-t-1$, we have

$$\beta^t(a_i) = \beta^t\beta^i(a_0) = \beta^{t+i}(a_0) = a_{t+i}.$$

Now let $n - t \le i \le n-1$. Write $i = n - t + k$, with $0 \le k \le t-1$. We have

$$\beta^t(a_i) = \beta^{t+i}(a_0) = \beta^{n+k}(a_0) = \beta^k\beta^n(a_0) = \beta^k(a_0) = a_k.$$

But this exactly agrees with the product of r-cycles given above. □

Now we prove the claims.

Suppose α is regular; say $\alpha = \sigma_0 \cdots \sigma_{t-1}$, where the σ_i are disjoint cycles of length r. Write

$$\sigma_i = (b_{i0}\, b_{i1}\, \ldots\, b_{i,r-1})$$

for each i. I want the product of the σ_i to look like the product of cycles in the claim. To do this, for $k = it + j$, $0 \le i \le t-1$, $0 \le j \le r-1$, define $a_k = b_{ij}$. I leave it as an exercise to show that we get the right side of (1). Then with β as in the claim, we get $\beta^t = \alpha$.

The reverse direction follows from (ii). For (ii), let $d = \gcd(r,k)$ and write $k = d\ell$. We have $\alpha^k = (\alpha^d)^\ell$. From the Claim, α^d is a product of d r/d-cycles. Observe that $\gcd(\ell, r/d) = 1$, so it suffices to show that if σ is an s-cycle ($s = r/d$) and $\gcd(\ell, s) = 1$, then σ^ℓ is also an s-cycle. I leave this as an exercise.

Part (iii) results immediately from (ii): if α is a p-cycle and p is prime, then for $k \in \mathbb{Z}$, $\gcd(k,p) = 1$ or p. Now apply (ii) to each case.

For (iv): we enumerate by cycle type. I will do S_5. We can have the identity, a 2-cycle, two 2-cycles, a 3-cycle, a 4-cycle, or a 5-cycle. There are

- one identity

- $\binom{5}{2}$ 2-cycles,
- $\binom{5}{2} \cdot \binom{3}{2}/2!$ products of two cycles (choose the first two cycle, then from the remaining 3 elements choose the second 2 cycle, then divide by 2 since this could have been done in the opposite order),
- $5 \cdot 4 \cdot 3/3$ 3-cycles,
- $5 \cdot 4 \cdot 3 \cdot 2/4$ 4-cycles, and
- $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1/5$ 5-cycles.

Adding these up, we get a total of 100 regular elements.

2.27 I first show by induction on k that $\alpha\beta^k = \beta^k\alpha$. The $k = 1$ case is by hypothesis. Suppose for some k, $\alpha\beta^k = \beta^k\alpha$. Then

$$\begin{aligned} \alpha\beta^{k+1} &= (\alpha\beta^k)\beta \\ &= (\beta^k\alpha)\beta \\ &= \beta^k(\alpha\beta) \\ &= \beta^k(\beta\alpha) \\ &= \beta^{k+1}\alpha. \end{aligned}$$

The claim follows by induction.

Now we show that $(\alpha\beta)^k = \alpha^k\beta^k$ by induction on k. The $k = 1$ case is clear. Assume the equality holds for some k. Then

$$\begin{aligned} (\alpha\beta)^{k+1} &= (\alpha\beta)^k\alpha\beta \\ &= (\alpha^k\beta^k)\alpha\beta \\ &= \alpha^k(\beta^k\alpha)\beta \\ &= \alpha^k(\alpha\beta^k)\beta \\ &= \alpha^{k+1}\beta^{k+1}. \end{aligned}$$

By induction, the claim holds.

The second one we did in class: $\alpha = (1\,2)$, $\beta = (2\,3)$. Then $\alpha^2\beta^2 = (1)$, while $(\alpha\beta)^2 = (3\,2\,1)$.

2.28 For (i), suppose α moves i, so $\alpha(i) = j \neq i$. Then $\alpha^{-1}(j) = i$. If we have $\alpha^{-1}(i) = i$, then since $i \neq j$, this would contradict the fact that α^{-1} is injective. Therefore $\alpha^{-1}(i) \neq i$, from which the claim follows. For the converse, reverse the roles of α and α^{-1}.

For (ii), we have $\beta = \alpha^{-1}$. Given $i \in \{1, 2, \ldots, n\}$, if α moves i, then by part (i), β also moves i. But α and β are disjoint, so cannot both move i. Therefore α does not move i. In other words, $\alpha(i) = i$. This holds $\forall i$, and hence α is the identity function. Since $\beta = \alpha^{-1}$, we have $\beta = (1)$ as well.

2.31 Suppose $\alpha(i) = j$. Since $n \geq 3$, there is some $k \neq i, j$. Let $\beta = (j\,k)$. By hypothesis, $\alpha\beta = \beta\alpha$. In particular,

$$\begin{aligned}(\beta\alpha)(i) &= \beta(\alpha(i)) \\ &= \beta(j) \\ &= k.\end{aligned}$$

Therefore $(\alpha\beta)(i) = k$. If $i \neq j$, then since also $i \neq k$, we have $\beta(i) = i$. This implies that $(\alpha\beta)(i) = \alpha(i) = j$, contradicting $j \neq k$. Therefore $i = j$, so i is a fixed point for α. Since i was arbitrary, α fixes everything, and hence is the identity.