HW 4 Selected Solutions

Prof. Shahed Sharif

2.22 Write $\alpha = (i_0\, i_1\, \ldots\, i_{r-1})$ with the i_k distinct. According to the hint, we would like to show that $\alpha^k(i_0) = i_k$ for $0 \leq k \leq r-1$. We do this by induction. The base case of $k = 0$ is clear. Suppose $\alpha^k(i_0) = i_k$ for some $0 \leq k \leq r-2$. Then

$$\begin{aligned} \alpha^{k+1}(i_0) &= \alpha(\alpha^k(i_0)) \\ &= \alpha(i_k) \\ &= i_{k+1}. \end{aligned}$$

By induction, the claim holds.

Next, we have $\alpha^r(i_0) = \alpha(\alpha^{r-1}(i_0) = \alpha(i_{r-1}) = i_0$. For $0 \leq k \leq r-1$, we have

$$\begin{aligned} \alpha^r(i_k) &= \alpha^r\alpha^k(i_0) \\ &= \alpha^{r+k}(i_0) \\ &= \alpha^k\alpha^r(i_0) \\ &= \alpha^k(i_0) \\ &= i_k. \end{aligned}$$

Here, the 4th equality follows from $\alpha^r(i_0) = i_0$ shown above, and the last equality follows from our claim from the hint.

Lastly, if $i \neq i_k$ for all k, then by definition of the cycle notation, $\alpha(i) = i$, and so in particular $\alpha^r(i) = i$. It follows that $\alpha^r = (1)$.

For (ii), observe that if $0 < k < r$, then $\alpha^k(i_0) = i_k \neq i_0$, so $\alpha^k \neq (1)$. The claim follows.

B. D_6 has order 6. The identity has order 1, the two nontrivial rotations have order 3, and every reflection has order 2. Therefore there are no elements of order 6.

C. The order of a is $\frac{n}{\gcd(a,n)}$. We first show that $\frac{n}{\gcd(a,n)}$ is a period. Let $d = \gcd(a, n)$; since $d \mid a$ and $d \mid n$, $\exists k, \ell \in \mathbb{Z}$ such that $a = kd$ and $n = \ell d$.Then $\ell = \frac{n}{\gcd(a,n)}$. We have

$$\begin{aligned} \ell a &= \ell k d \\ &= k\ell d \\ &= kn \\ &\equiv 0 \pmod{n}. \end{aligned}$$

Therefore ℓ is a period.

For the other direction, suppose m is a positive period, so $ma \equiv 0 \pmod{n}$. By the Euclidean algorithm, $\exists x, y \in \mathbb{Z}$ such that

$$ax + ny = d.$$

Multiplying through by m, we get

$$max + mny = md,$$

and since $ma \equiv 0 \pmod{n}$, we must have $md \equiv 0 \pmod{n}$. But this means that $n \mid md$. As $m > 0$, this means that $n \leq md$. But $n = \ell d$, so $\ell \leq m$. Thus ℓ is the smallest period, and hence is the order, as desired.