4.3 Consequences and applications of Lagrange's Theorem

Corollary 4.3.1. *Let H be a subgroup of a finite group G, and suppose $g \in G$. Then*

(i) $[G : H] = |G|/|H|$

(ii) $o(g)$ *divides* $|G|$

Proof. The proof of (i) is easy: by Lagrange, $|G| = [G : H] \cdot |H|$, therefore $|G|/|H| = [G : H]$.
To prove (ii), let $H = \langle g \rangle$. By Proposition 2.3.2 we know that $o(g) = |\langle g \rangle| = |H|$. By Lagrange, $|H| = o(g)$ divides the order of G. □

Example 4.3.2. Here are two example applications of Lagrange's Theorem that are basically the same.

1. The Dihedral group D_{10} does not contain an element of order 7.
   Proof: $|D_{10}| = 10 = 2 \cdot 5$. If D_{10} contained an element of order 7, then 7 would divide 10 which it does not.
2. The Dihedral group D_{10} does not contain a subgroup of order 7.
   Proof: if it did, then again $7 \big| 10$ which is false.

STOP Warning! The converse statement to Lagrange's Theorem does **not** hold—just because a number divides $|G|$, this does not mean that G has a subgroup of that order (the smallest couterexample has order 12 and is called the Alternating Group of degree 4. We will see this group later in the course).

Application of Lagrange's Theorem: how to understand the dihedral group

Recall $D_{2n} = \{e, \rho, \ldots, \rho^{n-1}, \sigma_1, \ldots, \sigma_n\}$ where the σ_i are reflections and ρ is the cycle $(1\,2\,\ldots\,n)$. Can we do better with the reflections?

First, notice that $|D_{2n}| = 2n$. Let $C = \langle \rho \rangle = \{e, \rho, \ldots, \rho^{n-1}\}$. Notice that $|C| = n$ and $C \leq D_{2n}$. By Lagrange's Theorem:

$$|D_{2n}| = [D_{2n} : C] \cdot |C|$$

Where $[D_{2n} : C]$ is the number of cosets of C in D_{2n}. Hence, $[D_{2n} : C] = \frac{|D_{2n}|}{|C|} = \frac{2n}{n} = 2$.
Let $\sigma = \sigma_1$. Since $\sigma \notin C$, we know (from Theorem 4.1.3) that $C \neq \sigma C$, and so the two cosets of C in D_{2n} must be C and σC. Hence

$$D_{2n} = C \cup \sigma C.$$

The reflections don't lie in C, so they must all lie in σC. This means that all the reflections are of the form $\sigma\rho^i$. Thus,

$$D_{2n} = \{e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}.$$

This is great, but we have a problem: how do we calculate things like $\rho\sigma$? It's not in the above list of elements in D_{2n}. What about even more complicated things, like $\rho\sigma\rho\sigma\rho^2\sigma$?

We start with $\rho\sigma$. It is easy to see that $\rho\sigma$ is not a translation (it reverses the label order on the corners), so it must be a reflection and therefore has order 2. Hence $(\rho\sigma)(\rho\sigma) = e$. Therefore,

$$\rho\sigma = (\rho\sigma)^{-1} = \sigma^{-1}\rho^{-1} = \sigma\rho^{-1} = \sigma\rho^{n-1}.$$

We can use this trick to calculate: $\rho^2\sigma, \rho^3\sigma, \ldots, \rho^{n-1}\sigma$.

Important summary: $D_{2n} = \{e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}$, with $\rho\sigma = \sigma\rho^{-1}$ and $\rho^n = e$ and $\sigma^2 = e$.
We can use the important summary above to easily work out combinations of rotations and reflections.

Question 4.3.3. Which element of $D_{2n} = \{e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}$ are the following equal to?

1. $\rho^3\sigma$ (Answer: $\rho^3\sigma = \rho^2\sigma\rho^{-1} = \rho\sigma\rho^{-2} = \sigma\rho^{-3} = \sigma\rho^{n-3}$)
2. $\rho\sigma\rho\sigma\rho^2\sigma$ (Answer: $\rho\sigma\rho\sigma\rho^2\sigma = \sigma\rho^{-1}\rho\sigma\rho^2\sigma = \sigma\sigma\rho^2\sigma = \rho^2\sigma = \rho\sigma\rho^{-1} = \sigma\rho^{-2} = \sigma\rho^{n-2}$)

Remark 4.3.4. What does σ look like in cycle notation? If σ is the line of reflection through the corner labelled 1, then as a permutation it is:

$$\sigma = (2\ \ n)(3\ \ n-1)(4\ \ n-2)\cdots$$