Warmup Q2‘a’ and Q7i

2‘a’) Write this permutation as product of

  i) disjoint cycles,

  ii) transpositions

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 1 & 8 & 2 & 3 & 5 \end{pmatrix}$$

.

7i) Find an element of maximal order in

$$((\mathbb{Z}/19)^\times, \cdot\ )$$

Permutations

- Permutation $\sigma \in S_n$ is a bijective function

$$\sigma \colon \{ 1, \ldots, n \} \to \{ 1, \ldots, n \}$$

- Multiplication is function composition. From right to left!

- As disjoint cycles, follow one input until you loop back. Notation

$$(a_1\ a_2\ \cdots\ a_k) := \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ a_2 & a_3 & \cdots & a_k & a_1 \end{pmatrix}$$

- As transpositions, use

$$(a_1\ a_2\ a_3\ \cdots\ a_k) = (a_1\ a_k) \cdots (a_1\ a_3)(a_1\ a_2)$$

Q2‘a’

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 1 & 8 & 2 & 3 & 5 \end{pmatrix}$$

i)
- $\rho(1) = 7$, $\rho(7) = 3$, $\rho(3) = 4$, $\rho(4) = 1$ back to start.
- This gives cycle $(1\ 7\ 3\ 4)$. Repeat for all elements.
- So $\rho = (1\ 7\ 3\ 4)(2\ 6)(5\ 8)$ as disjoint cycles.

ii)
- Apply $(a_1\ a_2\ a_3\ \cdots\ a_k) = (a_1\ a_k)\cdots(a_1\ a_3)(a_1\ a_2)$.
- This gives $(1\ 7\ 3\ 4) = (1\ 4)(1\ 3)(1\ 7)$. Repeat ...
- So $\rho = (1\ 4)(1\ 3)(1\ 7)(2\ 6)(5\ 8)$ as transpositions.

Order of elements

Definition (Order)

Order of $g \in G$ is smallest positive integer r with

$$g^r = e$$

Useful fact, which can save lots of work

Fact (via Lagrange)

If $\#G < \infty$, then

$$\text{order of } g \mid \#G$$

Q7i)

Element of maximal order in $G = ((\mathbb{Z}/19)^\times, \cdot\,)$?

- $(\mathbb{Z}/19)^\times = \{\, \overline{1}, \overline{2}, \dots, \overline{18}\,\}$.
- Possible element orders are 1, 2, 3, 6, 9, 18. (Divisors of $\#G = 18$.)
- Find order of $\overline{1}$, of $\overline{2}$, of $\overline{3}$, ... by computing powers
- Have $\overline{2}^2 = \overline{4} \neq \overline{1}, \quad \overline{2}^3 = \overline{8} \neq \overline{1}, \quad \overline{2}^6 = \overline{7} \neq 1, \quad \overline{2}^9 = \overline{18} \neq \overline{1}$.
- So order of $\overline{2}$ must be 18.

Maximal order in G is $18 = \#G$, so G is cyclic.
An element of maximal order is $\overline{2}$.