

1. Determine for which natural numbers we have  $n! > 2^n$  and prove it by induction.

```
create_list([n,n!,2^n],n,1,7);
```

```
[[1,1,2],[2,2,4],[3,6,8],[4,24,16],[5,120,32],[6,720,64],[7,5040,128]]
```

$$n! > 2^n \quad \text{for } n \geq 4$$

Pf. by induction on  $n$ :

Basics:  $n=4$ :  $n! = 24 > 16 = 2^4 \quad \checkmark$

Inductive step: let  $n > 4$ , assume  $\forall k < n \quad k! > 2^k$

In particular, since  $n-1 < n$  assume  $(n-1)! > 2^{n-1}$ ,

Then  $n! = n(n-1)! > n 2^{n-1} > 2 \cdot 2^{n-1} = 2^n \quad \checkmark$

2. Suppose  $\alpha, \beta \in \Sigma_n$  are permutations of  $\{1, 2, 3, 4, 5\}$  given by

$$\alpha(x) \begin{array}{c|ccccc} x & 1 & 2 & 3 & 4 & 5 \\ \hline & 3 & 2 & 4 & 1 & 5 \end{array}$$

$$\beta(x) \begin{array}{c|ccccc} x & 1 & 2 & 3 & 4 & 5 \\ \hline & 4 & 5 & 1 & 3 & 2 \end{array}$$

Find  $(\alpha\beta)^{-1}$  and  $\alpha^{-1}\beta^{-1}$

$$\underbrace{\beta^{-1}\alpha^{-1}}$$

$$\begin{array}{c|ccccc} x & 1 & 2 & 3 & 4 & 5 \\ \hline \alpha^{-1}(x) & 4 & 2 & 1 & 3 & 5 \\ \hline \beta^{-1}(x) & 3 & 5 & 4 & 1 & 2 \\ \hline \beta^{-1}(\alpha^{-1}(x)) & 1 & 5 & 3 & 4 & 2 \\ \hline \alpha^{-1}(\beta^{-1}(x)) & 1 & 5 & 3 & 4 & 2 \end{array}$$

Cycle notation:

$$\alpha = (134)$$

$$\beta = (143)(25)$$

$$\alpha^{-1} = (143)$$

$$\beta^{-1} = (134)(25)$$

$$\beta^{-1}\alpha^{-1} = (25)$$

$$\alpha^{-1}\beta^{-1} = (25)$$

3. Suppose  $G$  is a finite group and  $x \in G$ . Prove:

(a)  $x$  has finite order.

(b)  $x^n = e$  if and only if the order of  $x$  divides  $n$ .

(a) Since  $G$  is finite, by the pigeonhole principle

not all  $x^i, i \geq 1$  are distinct, so  $\exists i > j \quad x^i = x^j$

Then  $x^j = x^i = x^{i-j} x^j$ , so  $x^{i-j} = e$

By the well-ordering principle  $\{k > 0 : x^k = e\}$  has a minimum called the order of  $x$  (denoted  $|x|$ )

(b) Let  $m = |x|$

If  $m \mid n$ ,  $\exists q \in \mathbb{Z} \quad n = mq$ , so  $x^n = x^{mq} = (x^m)^q = e^q = e$

Conversely, suppose  $x^n = e$

By the division algorithm  $\exists ! q, r \in \mathbb{Z} \quad n = mq + r, \quad 0 \leq r < m$

$$r = n - mq \quad x^r = x^{n - mq} = x^n \cdot (x^m)^{-q} = e$$

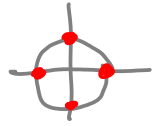
If  $r > 0$ , contradiction since  $r < m$

$\therefore r = 0$   $\checkmark$

4. Prove that the set of all complex fourth roots of unity  $H = \{z \in \mathbf{C} : z^4 = 1\}$  is a cyclic subgroup of  $\mathbf{C}^*$  of order 4

$$z^4 = 1 \Leftrightarrow z^4 - 1 = 0 \Leftrightarrow (z^2 - 1)(z^2 + 1) = 0$$

$$\Leftrightarrow (z-1)(z+1)(z-i)(z+i) = 0$$



Thus  $H = \{1, i, -1, -i\}$

Cayley table:

$\cdot$	1	$i$	-1	$-i$
1	1	$i$	-1	$-i$
$i$	$i$	-1	$-i$	1
-1	-1	$-i$	1	$i$
$-i$	$-i$	1	$i$	-1

$$H < \mathbf{C}^*$$

Pf: apply the subgroup test:

(i)  $1 \in H$

(ii) closure: Cayley table

(iii) inverses: every row has a 1

Fancy proof:  $H = \ker f$ , where  $f: \mathbf{C}^* \rightarrow \mathbf{C}^*$ ,  $f(z) = z^4$

$$[f(z_1 z_2) = (z_1 z_2)^4 = z_1^4 \cdot z_2^4 = f(z_1) \cdot f(z_2)]$$

$$H = \langle i \rangle = \{i^k : k \in \mathbb{Z}\} = \{i^0, i^1, i^2, i^3\} = \{1, i, -1, -i\}$$

Also  $H = \langle -i \rangle$

In fact  $\varphi: \mathbb{Z}_4 \rightarrow H$ ,  $\varphi(k) = i^k$  is an isomorphism:

Hom:  $\varphi(k_1 + k_2) = i^{k_1 + k_2} = i^{k_1} \cdot i^{k_2} = \varphi(k_1) \varphi(k_2)$

Surjective: by inspection

Since  $|\mathbb{Z}_4| = |H|$ ,  $\varphi$  is also injective