

$$S_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

$$\left\{ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

$$= \{ \leftarrow, \rightarrow, \nwarrow, \nearrow, \swarrow, \searrow \}$$

$$= \{ 1, (12), (23), (13), (123), (132) \}$$

Let S be a subset of G .

The subgroup of G generated by S is the subgroup $H \subseteq G$ such that

(a) $H \supseteq S$,

(b) If K is a subgroup of G and $K \supseteq S$ then $K \supseteq H$.

In English: H is the smallest subgroup of G containing S .

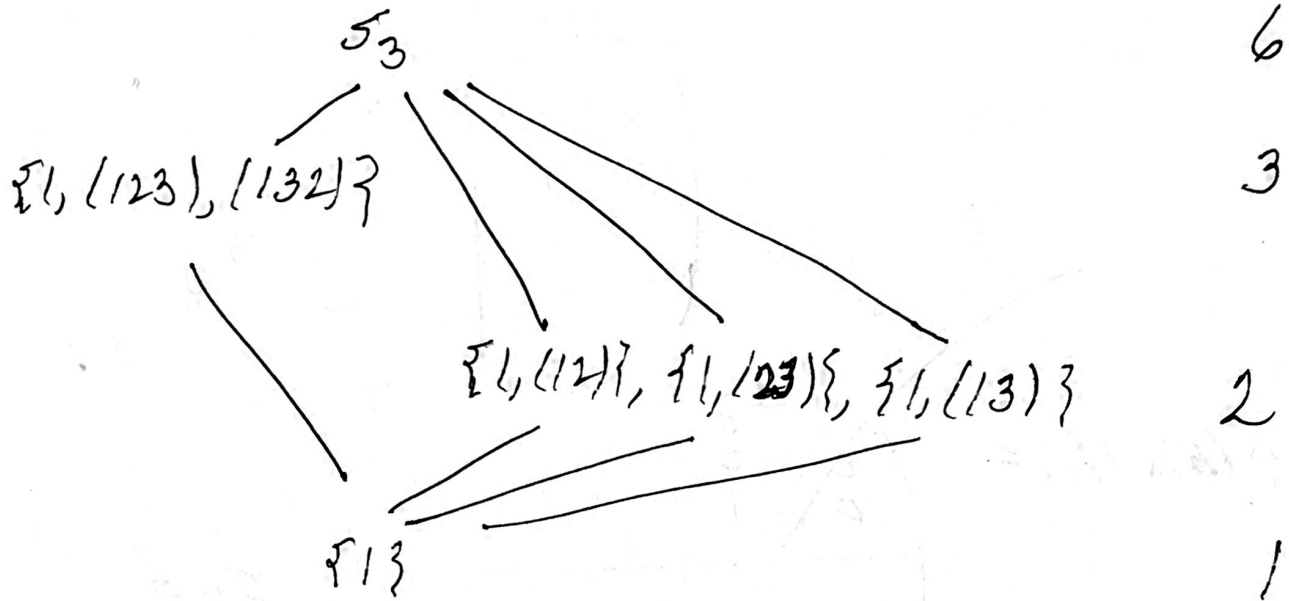
Note: The form of this definition is similar to one of the characterisations of \gcd and lcm . This is a "universal property".

Let G be a group. Let $g \in G$.

The order of g is the smallest $k \in \mathbb{Z}_{>0}$ such that

$$\underbrace{g \circ g \circ g \circ \dots \circ g}_{k\text{-times}} = e$$

Subgroups of S_3

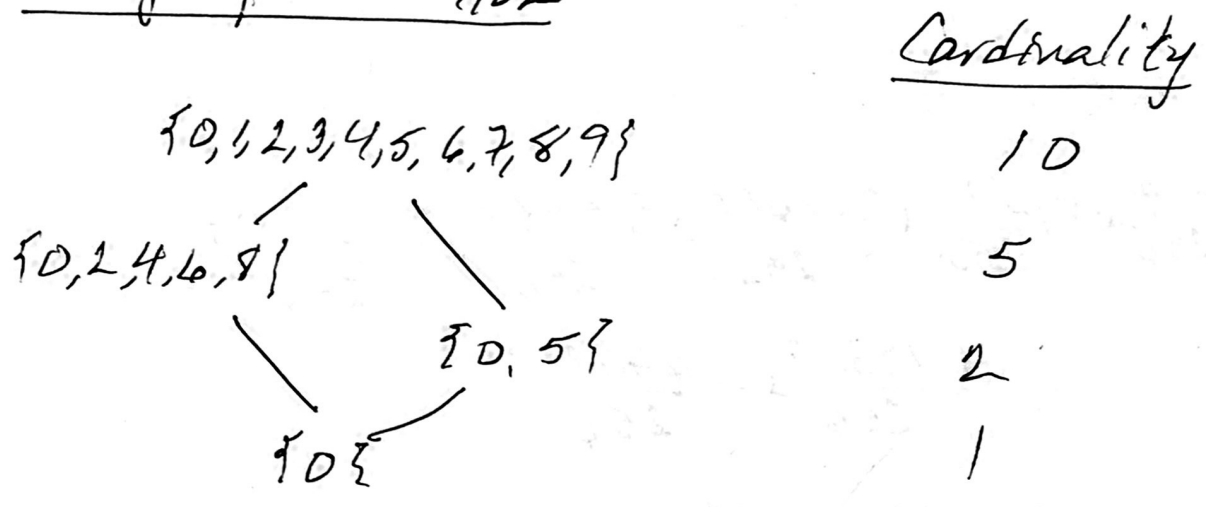


The group $\mathbb{Z}/10\mathbb{Z}$

$$\mathbb{Z}/10\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

- | | |
|-------------------------|---------------|
| $9+9+9+9+9+9+9+9+9+9=0$ | order(9) = 10 |
| $8+8+8+8+8=0$ | order(8) = 5 |
| $7+7+7+7+7+7+7+7+7+7=0$ | order(7) = 10 |
| $6+6+6+6+6=0$ | order(6) = 5 |
| $5+5=0$ | order(5) = 2 |
| $4+4+4+4+4=0$ | order(4) = 5 |
| $3+3+3+3+3+3+3+3+3+3=0$ | order(3) = 10 |
| $2+2+2+2+2=0$ | order(2) = 5 |
| $1+1+1+1+1+1+1+1+1+1=0$ | order(1) = 10 |
| $0=0$ | order(0) = 1 |

Subgroups of $\mathbb{Z}/10\mathbb{Z}$



The subgroup generated by 3 is

$$\begin{aligned} & \{0, 3, 3+3, 3+3+3, \dots, 3+3+3+3+3+3+3+3+3\} \\ & = \{0, 3, 6, 9, 2, 5, 8, 1, 4, 7\} \\ & = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = \mathbb{Z}/10\mathbb{Z} \end{aligned}$$

Proposition Let G be a group and let $g \in G$.

(a) Let $k \in \mathbb{Z}_{>0}$ and assume $\text{order}(g) = k$.

Then the subgroup generated by g is

$$\{1, g, g^2, \dots, g^{k-1}\} \text{ and}$$

$$\text{Card} \{1, g, g^2, \dots, g^{k-1}\} = \text{order}(g)$$

(b) Assume $\text{order}(g) = \infty$. Then the subgroup generated by g is

$$\{\dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \dots\}$$

and

$$\text{Card} \{\dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \dots\} = \text{order}(g).$$

Let G be a group. A cyclic subgroup of G is a subgroup generated by one element.