Basic facts about order of an element

Tuesday, June 29, 2021 3:29 PM

Let's recall that $o(g) = |\langle g \rangle|$. In particular, if G is a finite group, every element of G has finite order. Let's also recall that for a positive integer d, we have

$$o(g) = d \text{ exactly when } g^m = e_G \Leftrightarrow d \mid m.$$

We have also proved that $o(g^k) = \dfrac{o(g)}{\gcd(o(g), k)}$.

<u>Ex.</u> Suppose $f: G \to H$ is a group homomorphism. Then for every $g \in G$, $o(f(g)) \mid o(g)$.

<u>Pf.</u> Suppose $o(g) = d$. Then $g^d = e_G$. Hence

$$f(g^d) = f(e_G) = e_H. \qquad \text{(I)}$$

<u>Claim</u> $f(g^m) = f(g)^m$ for every integer m.

<u>Pf of Claim.</u> <u>$m=0$</u>. $f(g^0) = f(e_G) = e_H = f(g)^0$.

<u>$m>0$</u>. $f(g^m) = f(\underbrace{g \cdots g}_{m \text{ times}}) = \underbrace{f(g) \cdots f(g)}_{m \text{ times}} = f(g)^m$.

<u>$m<0$</u>. $f(g^m) = f((g^{-m})^{-1}) = f(g^{-m})^{-1} = (f(g^{-1})^m)^{-1}$ $\quad -m>0$

$$= (f(g)^{-1})^{-m} = f(g)^m.$$

By the above claim and (I), $f(g)^d = e_H$. Hence $o(f(g)) \mid d$. ∎

Basic facts about order of an element

Tuesday, June 29, 2021 3:29 PM

Ex. Suppose $f: G \to H$ is a group isomorphism. Then for every $g \in G$, $o(f(g)) = o(g)$.

Pf. We can use the previous example to show this. But here I use only the claim in the previous example. We have that for every integer m, $f(g^m) = f(g)^m$. (I) Hence f gives us a group homomorphism from $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ to $\langle f(g) \rangle = \{f(g)^m \mid m \in \mathbb{Z}\}$,

$$\bar{f}: \langle g \rangle \to \langle f(g) \rangle, \quad \bar{f}(g^m) := f(g^m).$$

By (I), $\bar{f}$ is a surjective. Because f is an isomorphism, it is injective. Hence $\bar{f}$ is injective. Therefore $\bar{f}$ is a bijection. Hence $|\langle g \rangle| = |\langle f(g) \rangle|$. Since $|\langle g \rangle| = o(g)$ and $|\langle f(g) \rangle| = o(f(g))$, we conclude that $o(g) = o(f(g))$.

Ex. Suppose $(G, \cdot)$ is a group and $x, y \in G$. Then $\forall m \in \mathbb{Z}$,

$$(x \cdot y \cdot x^{-1})^m = x \cdot y^m \cdot x^{-1} \quad \text{and} \quad o(x \cdot y \cdot x^{-1}) = o(y).$$

Pf. Both of these follow from the fact that the conjugation $c_y: G \to G$, $c_y(x) = y \cdot x \cdot y^{-1}$ by y is a group isomorphism. ∎

Order of permutations

Tuesday, June 29, 2021 3:29 PM

Here we find order of a permutation given its cycle decomposition. We start with a cycle. Suppose

$$\sigma = (a_0, a_1, \ldots, a_{m-1})$$

Then $a_0 \xmapsto{\sigma} a_1 \xmapsto{\sigma} \cdots \xmapsto{\sigma} a_{m-1}$, and so each time we apply σ to a_j we add its index by 1. But we add modulo m. Hence after applying σ^i to a_j we get a_{i+j} where $i+j$ is considered modulo m.

Therefore $\sigma^i = \mathrm{id}. \iff i+j \equiv j \pmod{m}$ for every j

$$\iff i \equiv 0 \pmod{m}$$

$$\iff m \mid i.$$

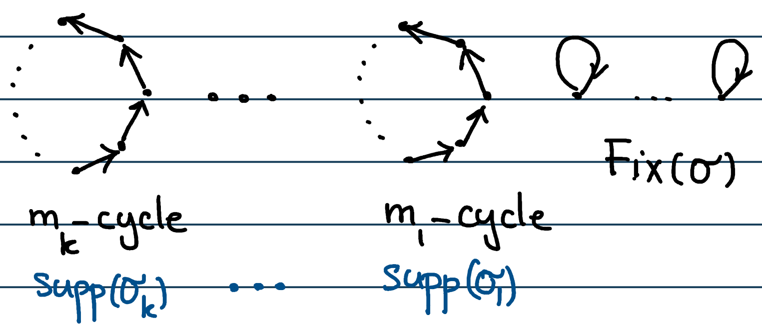
Hence $o(\sigma) = m$. (Order of an m-cycle is m.)

- Now suppose $\sigma_1 \sigma_2 \cdots \sigma_k$ is a cycle decomposition of σ and σ_i is an m_i-cycle. Since σ_i's are disjoint, they commute. Hence, for every integer m,

$\sigma^m = (\sigma_1 \sigma_2 \cdots \sigma_k)^m = \sigma_1^m \sigma_2^m \cdots \sigma_k^m$. Let's recall that

Order of permutations

Tuesday, June 29, 2021 3:29 PM



For every x in $\mathrm{Supp}(\sigma_i)$ we have $\sigma(x) = \sigma_i(x)$ and $\sigma_i(x) \in \mathrm{Supp}(\sigma_i)$.
Therefore for $x \in \mathrm{Supp}(\sigma_i)$ we have $\sigma^\ell(x) = \sigma_i^\ell(x)$ for every integer ℓ. (On $\mathrm{Supp}(\sigma_i)$, σ and σ_i permute the same way.) Hence $\sigma^\ell = \mathrm{id}.$ implies that $\sigma_i^\ell = \mathrm{id}.$ for every i. Thus $o(\sigma_i) \mid \ell$. We conclude that

$$\sigma^\ell = \mathrm{id}. \implies m_i \mid \ell \text{ for every } i.$$

This implies that the least common multiple of m_i's divide ℓ (One can prove this by induction using Euclid's lemma)

Thus $\sigma^\ell = \mathrm{id}. \implies \mathrm{l.c.m.}(m_1, \dots, m_k) \mid \ell$. (I)

- Suppose $\mathrm{lcm}(m_1, \dots, m_k) \mid \ell$. Then $\sigma_i^\ell = \mathrm{id}.$ for every i as $o(\sigma_i) \mid \ell$. Hence $\sigma^\ell = \sigma_1^\ell \sigma_2^\ell \cdots \sigma_k^\ell = \mathrm{id}.$ (II)

(I) and (II) imply that $\sigma^\ell = \mathrm{id}. \iff \mathrm{lcm}(m_1, \dots, m_k) \mid \ell$.

Therefore $o(\sigma) = \mathrm{lcm}(m_1, \dots, m_k)$.

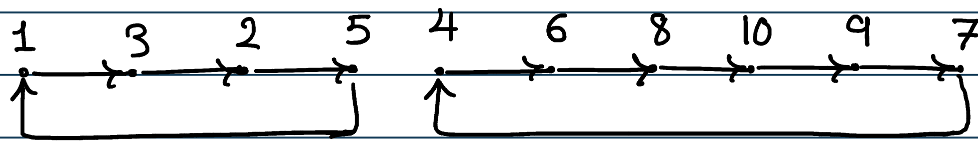
Order of permutations

Tuesday, June 29, 2021 3:29 PM

Ex. Find $o(\sigma)$ where $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 2 & 6 & 1 & 8 & 4 & 10 & 7 & 9 \end{pmatrix}$

Solution. We start by finding a cycle decomposition of σ.

We follow the flow



Hence $\sigma = \underbrace{(1,3,2,5)}_{4\text{-cycle}} \underbrace{(4,6,8,10,9,7)}_{6\text{-cycle}}$, and so

$o(\sigma) = \operatorname{lcm}(4,6) = 12$.

Ex. Is σ odd or even?

Solution. A 4-cycle is odd and an 6-cycle is odd.

Hence $\operatorname{sgn}(\sigma) = \operatorname{sgn}(1,3,2,5)\, \operatorname{sgn}(4,6,8,10,9,7)$

$= (-1)(-1) = 1$, and so

σ is even.

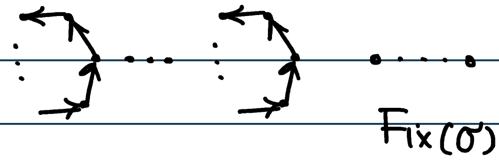
Ex. Suppose p is prime and $\sigma \in S_p$ is an element of order p. Then σ is a p-cycle.

Pf. Suppose $\sigma_1 \sigma_2 \cdots \sigma_k$ is a cycle decomposition of σ and σ_i is an m_i-cycle. Since $\sigma_1, \dots, \sigma_k \in S_p$ are disjoint

Order of permutations

Tuesday, June 29, 2021 3:29 PM

cycles, $m_1 + m_2 + \cdots + m_k \le p$.



Since $o(\sigma) = p$, we have

(There are a total of p points.)

$\operatorname{lcm}(m_1, \ldots, m_k) = p$. Therefore

$m_i \mid p$ for every i, and so $m_i = 1$ or p for every i.

Since $m_i > 1$, we conclude that $m_i = p$ for every i.

Because $m_1 + \cdots + m_k \le p$ and $m_i = p$ for every i, we

deduce that $\underline{\underline{k=1}}$, and so σ is a p-cycle.

<u>Ex.</u> What is $\max\{o(\sigma) \mid \sigma \in S_7\}$?

<u>Solution.</u> Suppose $\sigma_1 \cdots \sigma_k$ is a cycle decomposition of σ

and σ_i is an m_i-cycle for every i. Then

$o(\sigma) = \operatorname{lcm}(m_1, \ldots, m_k)$ and $m_1 + m_2 + \cdots + m_k \le 7$.

We write 7 as a sum of (non-decreasing) positive

integers, and take the <u>lcm</u> of these integers. Finally we

take the maximum of these lcm's.

7	6+1	5+2	5+1+1	4+3	4+2+1	4+1+1+1	The rest
$\rightsquigarrow$ 7	$\rightsquigarrow$ 6	$\rightsquigarrow$ 10	$\rightsquigarrow$ 5	$\rightsquigarrow$ 12	$\rightsquigarrow$ 4	$\rightsquigarrow$ 4	

Order of permutations

Tuesday, June 29, 2021 3:29 PM

have integers 1, 2, and 3. Hence the lcm of the rest is at most 6. Hence the maximum order of elements in S_7 is 12. For instance, $o((1,2,3)(4,5,6,7)) = 12$.