A few comments on orders of groups and elements

September 2023, Matt Valeriote

This brief note reproduces some of the claims made during the lecture on Tuesday, 26 September, but in a slightly more organized manner.

- Recall that for G a group, $|G|$, called the order of G, denotes the number of elements in G, if G is a finite set, and is ∞ otherwise.

- For $a \in G$, $|a|$, called the order of the element a, is the least natural number $n > 0$ such that $a^n = e$. If no such n exists, then we write $|a| = \infty$ and say that the order of a is infinite.

- For $a \in G$, $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. We have seen that $\langle a \rangle$ is always a subgroup of G, and is referred to as the cyclic subgroup of G generated by a. If $G = \langle a \rangle$ for some $a \in G$, then G is said to be a cyclic group and that a is a (cyclic) generator of G.

- Claim: For $a \in G$ and $m \in \mathbb{N}$, if $|a| = m$ then $\langle a \rangle = \{e, a^1, a^2, \ldots, a^{m-1}\}$ and $|\langle a \rangle| = m$. If $|\langle a \rangle| = m$ then $|a| = m$.

  Proof: Suppose that $|a| = m$ and show that $\langle a \rangle = \{e, a^1, a^2, \ldots, a^{m-1}\}$ and that this set has size exactly m. Certainly the set on the right hand side is contained in $\langle a \rangle$. To show equality, let $b \in \langle a \rangle$. Then $b = a^k$ for some $k \in \mathbb{Z}$. By the Division Algorithm, there are $q, r \in \mathbb{Z}$ with $k = qm + r$ and $0 \leq r < m$. Then

  $$b = a^k = a^{qm+r} = (a^m)^q \circ a^r = e^q \circ a^r = a^r,$$

  showing that b is a member of the set on the right hand side.

  So, this set has at most m elements. To see that it has exactly m elements, suppose that $i,\ j < m$, with $i \leq j$ and $a^i = a^j$. Then $a^{j-i} = e$ and so $j - i = 0$, and hence $i = j$, since $j - i < m$ and $|a| = m$.

  Now, suppose that $|\langle a \rangle| = m$. Then there must be natural numbers $k < p$ with $a^k = a^p$, for if not, then $\langle a \rangle$ would be infinite. Then $a^{p-k} = e$ which implies that $|a| = q$ for some natural number q. By the first part of this claim, it follows that $q = m$ and so $|a| = m$.

- From the Claim it follows that if G is a group with $|G| = m$ for some $m > 0$, then G is cyclic if and only if G has an element of order m. In this case, any element of order m in G is a generator of G.