

- (1) Prove that the order of any group element is equal to the order of its inverse.

By definition of order, $o(a) = |\langle a \rangle|$, and by definition of generation, $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.
 Note that $\{a^n : n \in \mathbb{Z}\} = \{a^{-n} : n \in \mathbb{Z}\}$, because \mathbb{Z} contains exactly the same positive as negative values. Thus $\langle a \rangle = \langle a^{-1} \rangle$, and since a and a^{-1} generate groups of the same size, they have the same order.

- (2) Prove that the order of a^5 is less than or equal to the order of a for any element a of any finite group.

Well, any power of a^5 is also a power of a , so $\langle a^5 \rangle \leq \langle a \rangle$. This tells us not only that $o(a^5) \leq o(a)$, but even that $o(a^5) \mid o(a)$ (by Lagrange's Theorem, the order of a subgroup divides the order of the group).

- (3) Give an example of a group and an element a for which $1 < o(a^2) < o(a)$.

Possibly the easiest example is $G = \mathbb{Z}_4$. This is a cyclic group with $\langle 1 \rangle = \{0, 1, 2, 3\} = G$ so $o(1) = 4$. But $\langle 2 \rangle = \{0, 2\}$. This is an ADDITIVE group, so the meaning of a^2 is $a \star a = a + a$. Thus the "square" of 1 is 2, but it has a lower order.

If you find the additive/multiplicative thing confusing, we can replace this by the example $G = \langle i \rangle$ in \mathbb{C}^\times . Here $\langle i \rangle = \{1, i, -1, -i\}$ so $o(i) = 4$, and here $i^2 = -1$, so $o(i^2) = 2$. (This example is isomorphic to the last one!)