Name: Solutions

Problem 1 (2 points). Define a *group* $(G, \cdot)$.

A group $(G, \cdot)$ is a set with a binary operation s.t. $\cdot$ is associative, has an identity, and every element has an inverse.

Problem 2 (4 points). Let G be a group, and $g \in G$ be an element of order t. Show that if $t = ab$ for some positive integers a, b, then the order of g^a is b.

First, note that $(g^a)^b = g^{ab} = g^t = e$, so the order of g^a is at most b. On the other hand, if $(g^a)^c = e$, ~~then~~ with $c > 0$, ~~then~~ $g^{ac} = e$, ~~so~~ $ac \geq t$, so $c \geq b$. Thus, b is the order of g^a.

Problem 3 (4 points). Let G be a finite group of order n (i.e., G has n distinct elements), and let $g \in G$. Show that the order of g is less than or equal to n.

We showed last time ~~that~~ $|\langle g \rangle| = \mathrm{ord}(g)$. Since $\langle g \rangle \leq G$, $\mathrm{ord}(g) = |\langle g \rangle| \leq |G| = n$.