Back to finite groups: heading for the Sylow theorems.

We have already seen that if G is a finite group, then the order of each element of G is a divisor of the order of G.

(Recall why: $g \in G$ generates a subgroup $e, g, \ldots, g^{\operatorname{ord} g - 1}$ with $\operatorname{ord}(g)$ elements.

G = disjoint union of (right) cosets of this subgroup, which are pairwise disjoint and contain $\operatorname{ord}(g)$ elements).

The converse is not true in general (e.g. S_3 has order 6, $6 | 6$ but there is no element of order 6 since $S_3 \ncong \mathbb{Z}_6$).

But there is a kind of partial converse in some cases: Look at abelian first:

If G is an abelian finite group and if p is a prime that divides $\operatorname{ord}(G)$ then $\exists\, g \in G$ of order p.

Proof by induction of $|G|$ ($\neq 1$).

If $G \neq \mathbb{Z}_p$ then G has nontrivial ($\neq \emptyset, \neq G$) subgroups. ($G \cong \mathbb{Z}_p$: result holds trivially)

If H is a proper subgroup with order divisible by p, then H has an element of order p

(inductively) and so we assume

$p \nmid$ order H. Then inductively on order

H has an element of order q for some prime $q \neq p$, say $y \in H$. Then

$G/$ subgrp generated by y has order divisible by p. So $G/$ subgrp generated by y has element of order p. Say $\bar{z}$ with $\bar{z}^p = \mathrm{id} \in$ $\overline{G/\text{subgr.}}$

So $\exists\, z \in G \ni z \to \bar{z}$ under

$G \to G/$ subgrp generated by y. Then

$z^p = y^i$ some i. Hence $(z^q)^p = (y^i)^p = (y^p)^i = e$

So z^q has order p. $\square$

Example: $\mathbb{Z}_6$ has elements of orders 2 and 3.

Now we want to extend this to groups that are not necessarily abelian.

Theorem: If G is a finite group and p is a prime such that $p \mid \operatorname{ord}(G)$, then G has an element of order p.

Example: S_3 has elements of orders 2 and 3 ($\operatorname{ord} S_3 = 6$)

Proof: For each element g in G we consider the "conjugacy class" of g

notation $= [g] \overset{\text{def}}{=} \{ g_1^{-1} g g_1 : g_1 \in G \}$

Note that two conjugacy classes are either disjoint or identical (conjugacy $\overset{\text{def}}{=}$ $g \sim g' \Leftrightarrow \exists g_1 \ni g_1^{-1} g g_1 = g'$ is an equivalence relation: exercise).

Also the number of elements in $[g]$ = index of the "normalizer of g"

[normalizer of $g = \{ g_1 : g_1^{-1} g g_1 = g \}$]

This is just our "orbit" idea all over again:

conjugacy class of g = orbit of g under conjugation action and number of elements in an orbit = $\operatorname{ord}(G) / \operatorname{ord}$ (stabilizer of g in G acting by conjugation)

Now think about G = union of conjugacy classes.

$\{e\}$ is a conjugacy class. So is $\{z\}$ if z commutes with every element of G.

But these are the only ones containing only one element.

The other conjugacy classes correspond to normalizers that are proper subgroups.

Now returning to $|G|$ divisible by p:

If G has a proper subgroup H with order divisible by p, then H has an element of order p inductively. But if H has no proper subgroup with order divisible by p then every conjugacy class that is not a single element (so normalizer = whole group) contains a number of elements divisible by p

(since number $= \mathrm{ord}(G)/\mathrm{ord}(\text{normalizer})$ so if $p \nmid \mathrm{ord}(\text{normalizer})$ then $p \mid$ number since $p \mid \mathrm{ord}(G)$)

So the number of elements with no conjugate other than the element itself is divisible by p!

So "center" of G [$= Z(G)$, notation] has order divisible by p.

But the center $Z(G)$ is abelian. So by previous, $Z(G)$ contains an element of order p. and this element is of course in G □