March 26th

<u>Recall</u>: Let G be a finite group and $p \mid |G|$. Then G has an element of order p.

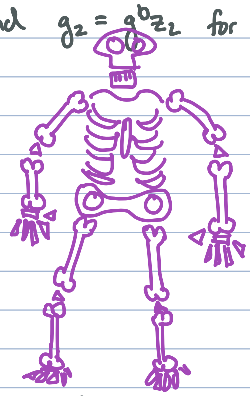
<u>Corollary</u>: Let G be a group of order p^n for $n \geq 1$, p prime. Then $Z(G) \neq \{e_G\}$.
(There exists atleast one nontrivial element that commutes)

Proof. If $Z(G) = G$, we are done. If $Z(G) \neq G$, take $x \in G$, $x \notin Z(G)$.
We know $C_G(x)$ is a proper subgroup of G. So $|G|/|C_G(x)| \mid |G|$ and $|G|/|C_G(x)| \neq 1$ (since proper), so $|G|/|C_G(x)| = p^k$ for some $1 \leq k \leq n$.
Recall that $|G| = |Z(G)| + \sum_{i=1}^{k} |G|/|C_G(x)|$, so $p^n = |Z(G)| + p^{k_i}$. We then have that $p(p^{n-1} + p^{k_i - 1}) = |Z(G)|$, hence $p \mid |Z(G)|$ Therefore $Z(G) \neq \{e_G\}$. □

<u>Corollary</u>: Let G be a group with $|G| = p^2$, p prime. Then G is abelian and $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. If $Z(G) = G$, then G is abelian. If $Z(G) \neq G$, then $|Z(G)| \mid p^2$ and $|Z(G)| \neq 1$ and $|Z(G)| \neq p^2$ b/c $Z(G) \neq G$. Thus $|Z(G)| = p$.
We also have $Z(G) \trianglelefteq G$, so $G/Z(G)$ is a group. Moreover, $|G/Z(G)| = |G|/|Z(G)| = p$.
Thus $G/Z(G) = \langle gZ(G) \rangle$ (because every group of prime power is cyclic) for some $g \in G$.
Let $g_1, g_2 \in G$. We can write $g_1 = g^a z_1$ and $g_2 = g^b z_2$ for some $a, b \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$. We have that:

$$\begin{aligned} g_1 g_2 &= g^a z_1 g^b z_2 \\ &= g^a g^b z_1 z_2 \\ &= g^{a+b} z_1 z_2 \\ &= g^b g^a z_2 z_1 \\ &= g^b z_2 g^a z_1 \\ &= g_2 g_1. \end{aligned}$$



Thus G is abelian. If G has an element of order p^2, then G is cyclic. So $G \cong \mathbb{Z}/p^2\mathbb{Z}$.
Assume G does not have an element of order p^2. Let $x \in G$, $x \neq e_G$. Then $|x| = p$.
Note $\langle x \rangle \subsetneq G$, so take $y \in G \setminus \langle x \rangle$. Then y has order p. Define $\langle x, y \rangle = \{x^a y^b : a, b \in \mathbb{Z}\}$. This is a subgroup b/c G is abelian. We have that $\langle x \rangle \subsetneq \langle x, y \rangle \leq G$. So $|\langle x, y \rangle| = p^2$; i.e., $G = \langle x, y \rangle$.
Define $\varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \longrightarrow G$ by $(a,b) \mapsto x^a y^b$. This is an isomorphism □

<u>Example</u>: Let $X = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
Let $G = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}) : \sigma(x) = x \ \forall x \in \mathbb{Q},$
σ bijective, $\sigma(x+y) = \sigma(x) + \sigma(y)$, $\sigma(xy) = \sigma(x)\sigma(y).\}$.
We can show that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is a group under function composition.
What are the elements of G? Note if $\sigma \in G$, then
$$\begin{aligned} 2 &= \sigma(2) \\ &= \sigma(\sqrt{2}^2) \\ &= \sigma(\sqrt{2})^2 \end{aligned}$$

Thus $\sigma(\sqrt{2}) = \pm\sqrt{2}$. We have $\sigma(a+b\sqrt{2}) = \sigma(a) + \sigma(b)\sigma(\sqrt{2})$

$$= a + b\sigma(\sqrt{2}).$$

Thus there are only two possible maps:

$$\sigma_0(a+b\sqrt{2}) = a+b\sqrt{2}$$
$$\sigma_1(a+b\sqrt{2}) = a-b\sqrt{2}$$

So $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma_0, \sigma_1\} \cong \mathbb{Z}/2\mathbb{Z}$. This is known as the Galois Group.

<u>Definition</u>: Let G be a group, p prime.

1) A group of order p^n, $n \geq 1$ is called a <u>p-group</u>.
2) Let $|G| = p^n m$ w/ $p \nmid m$. A subgroup of G of order p^n is called a <u>p-Sylow subgroup of G</u>. The collection of p-sylow subgroups is denoted $\mathrm{Syl}_p(G)$ and $n_p(G) = \#\mathrm{Syl}_p(G)$.

<u>Theorem</u>: (Sylow's Theorem) Let G be a group with $|G| = p^n m$ and $p \nmid m$.

1) If $1 \leq k \leq n$, then G has a subgroup of order p^k. In particular, $\mathrm{Syl}_p(G) \neq \emptyset$.
2) If $P \in \mathrm{Syl}_p(G)$ and Q is any p-subgroup of G, then there exists an element $g \in G$ so that $Q \leq gPg^{-1}$. In particular, all p-Sylow subgroups are conjugate.
3) We have $n_p(G) \equiv 1 \pmod{p}$. Moreover,

$$n_p(G) = \frac{G}{|N_G(P)|} \text{ for any } P \in \mathrm{Syl}_p(G),$$

where $N_G(P) = \{g \in G : gPg^{-1} = P\}$. Furthermore, $n_p(G) \mid m$.