# GROUPS ACTING ON A SET 

MATH 435 SPRING 2012
NOTES FROM FEBRUARY 27TH, 2012

## 1. Left group actions

Definition 1.1. Suppose that $G$ is a group and $S$ is a set. A left (group) action of $G$ on $S$ is a rule for combining elements $g \in G$ and elements $x \in S$, denoted by $g . x$. We additionally require the following 3 axioms.
(0) $g \cdot x \in S$ for all $x \in S$ and $g \in G$
(1) e. $x=x$ for all $x \in S$.
(2) $g_{1} \cdot\left(g_{2} \cdot x\right)=(g 1 g 2) \cdot x$ for all $x \in S$ and $g_{1}, g_{2} \in G$.

It is critical to note that in (2) above, $g_{1} \cdot\left(g_{2} \cdot x\right)$ has two actions of $G$ on elements of $S$. On the other hand $\left(g_{1} g_{2}\right) \cdot x$ has one multiplication in the group $g_{1} g_{2}$ and then one action of an element of $G$ on $S$.

Now we present an example.
Example 1.2. Suppose that $S$ is any set and consider $G$ to be any subgroup of $A(S)$. Then $G$ acts on $S$ as follows. For each $f \in G \subseteq A(S)$ and each $x \in S$, we define

$$
f . x=f(x) \in S
$$

Note that $f: S \rightarrow S$ is a (bijective) function since $f \in A(S)$. Thus this makes sense and condition (0) is verified. For condition (1), note that $e \in G$ is the identity function id :S $\rightarrow S$, and id $. x=\operatorname{id}(x)=x$ as desired. Finally we verify (2), note that if $f, g \in G$, then $f \cdot(g \cdot x)=f(g \cdot x)=$ $f(g(x))=(f \circ g)(x)=(f g) \cdot x$ as desired.

We now consider the same example in a slightly more explicit framework.
Example 1.3. Suppose that $G=S_{4}$, the group of permutations on the set $S=\{1,2,3,4\}$. We illustrate the action of $G$ on $S$ as in the following examples:
(a) $(12)(34) .3=4$
(b) $(12)(34) \cdot 2=1$
(c) $(1234) .2=3$
(d) $(132)(12) .2=3$
(e) $(132)(12) .4=4$

Finally, we give an example of matrices acting on vectors.
Example 1.4. Suppose that $G$ is the group of $2 \times 2$ matrices, $\left\{\left.\left[\begin{array}{rr}\cos \theta & \sin \theta \\ -\sin \theta & \cos \theta\end{array}\right] \right\rvert\, \theta \in \mathbb{R}\right\}$, under matrix multiplication. These are the set of matrices which, when multiplying a column vector $\mathbf{v}$, rotates $\mathbf{v}$ clockwise by $\theta$. This gives us an action of $G$ on $\mathbb{R}^{2}$, by $A . \mathbf{v}=A \mathbf{v}$. For example, if $\theta=\pi / 2$ and $\mathbf{v}=\left[\begin{array}{l}1 \\ 0\end{array}\right]$, then consider the matrix acting on the vector

$$
\left[\begin{array}{rr}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta
\end{array}\right] \cdot\left[\begin{array}{l}
1 \\
0
\end{array}\right]=\left[\begin{array}{rr}
0 & 1 \\
-1 & 0
\end{array}\right]\left[\begin{array}{l}
1 \\
0
\end{array}\right]=\left[\begin{array}{c}
0 \\
-1
\end{array}\right]
$$

It is easy to verify that this really is a group action. Note that the identity matrix is in $G$ (it corresponds to $\theta=0$ ), and the identity matrix sends vectors to themselves. Also, note that $B \cdot(A . \mathbf{v})=B(A \mathbf{v})=(B A) \mathbf{v}=(B A) . \mathbf{v}$ which completes the proof.

We conclude with several more examples.
Example 1.5 (Group acting on itself by multiplication). Every group $G$ acts on itself as follows, set $G=G$ and $S=G$. Then for $g \in G$ and $x \in S=G$, we define $g . x=g x \in S=G$. I will leave it to you to verify that this is a group action.

Example 1.6 (Group acting on itself by conjugation). Every group $G$ acts on itself in a different way. Again set $G=G$ and $S=G$. Then for $g \in G$ and $x \in S$ we define $g \cdot x=g x g^{-1} \in S=G$. It is clear that this rule satisfies condition (0). Likewise (1) is easy since $e . x=e x e^{-1}=x$. Finally we come to (2), and so we suppose that $g, h \in G$ and $x \in S=G$. Then

$$
g \cdot(h \cdot x)=g \cdot\left(h x h^{-1}\right)=g\left(h x h^{-1}\right) g^{-1}=(g h) x\left(h^{-1} g^{-1}\right)=(g h) x(g h)^{-1}=(g h) \cdot x
$$

as desired.
Note that if $G$ is Abelian, then this group action is trivial, in other words $g \cdot x=x$ for all $g \in G$ and $x \in S$.

## 2. Right group actions

Definition 2.1. Suppose that $G$ is a group and $S$ is a set. A right (group) action of $G$ on $S$ is a rule for combining elements $g \in G$ and elements $x \in S$, denoted by $x . g$. We additionally require the following 3 axioms.
(0) $x . g \in S$ for all $x \in S$ and $g \in G$
(1) $x . e=x$ for all $x \in S$.
(2) $\left(x \cdot g_{2}\right) \cdot g_{1}=x \cdot\left(g_{2} g_{1}\right)$ for all $x \in S$ and $g_{1}, g_{2} \in G$.

Remark 2.2. Left group actions are not really very different from right group actions. The only difference occurs in axiom (2).

- For left group actions, applying $g_{2}$ to an element and then applying $g_{1}$ to the result is the same as applying $g_{1} g_{2} \in G$.
- For right group actions applying $g_{2}$ and then $g_{1}$ is the same as applying $g_{2} g_{1} \in G$.

We'll only give one example of a right group action (besides the Rubik's cube example, which as we wrote things is a right group action). We'll do matrices multiplying vectors from the right.
Example 2.3. Suppose that $G$ is the group of $2 \times 2$ matrices, $\left\{\left.\left[\begin{array}{rr}\cos \theta & \sin \theta \\ -\sin \theta & \cos \theta\end{array}\right] \right\rvert\, \theta \in \mathbb{R}\right\}$, under matrix multiplication. Set $S=\mathbb{R}^{2}$ to be the set of row vectors $\left[\begin{array}{ll}x & y\end{array}\right]$. We have a right action of $G$ on $S$ defined by matrix multiplication times a vector:

$$
\mathbf{v} \cdot A=\mathbf{v} A
$$

for $\mathbf{v} \in \mathbb{R}^{2}$ and $A \in G$. If $A$ corresponds to $\theta$, then this action rotates a vector $\mathbf{v}$ by $\theta$ radians counter-clockwise. For example, set $\theta=\pi / 2$ and set $\mathbf{v}=\left[\begin{array}{ll}1 & 0\end{array}\right]$. For example, consider

$$
\left[\begin{array}{ll}
1 & 0
\end{array}\right] \cdot\left[\begin{array}{rr}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta
\end{array}\right]=\left[\begin{array}{ll}
1 & 0
\end{array}\right]\left[\begin{array}{rr}
0 & 1 \\
-1 & 0
\end{array}\right]=\left[\begin{array}{ll}
0 & 1
\end{array}\right]
$$

Just as before it is easy to see that this is a right group action.
I want to do one more type of example that wasn't done earlier.

Example 2.4 (A group acting on a set of cosets). Suppose that $G$ is a group and $H$ is a subgroup (not necessarily normal). Consider the set $S=\{H a \mid a \in G\}$ of right cosets of $H$. Then $G$ acts on $S$ by right multiplication, in other words, we define:

$$
(H a) \cdot g=H(a g)
$$

for $g \in G$ and $H a \in S$. First we should verify that this is well defined, so suppose that $H a=H a^{\prime}$, then $a^{\prime} a^{-1} \in H$. Now, we need to show that $H(a g)=H\left(a^{\prime} g\right)$ for any $g \in G$. But $a^{\prime} a^{-1} \in H$ so that $a^{\prime} g=\left(a^{\prime} a^{-1}\right)(a g) \in H(a g)$ so that $a^{\prime} g \in H(a g)$. But certainly $H\left(a^{\prime} g\right)$ also contains $e\left(a^{\prime} g\right)=a^{\prime} g$. Thus the two cosets $H(a g)$ and $H\left(a^{\prime} g\right)$ have the elements $a^{\prime} g$ in common. This proves that $H(a g)=H\left(a^{\prime} g\right)$ since cosets are either equal or disjoint.

Now that we have shown that this rule is well defined, we need to prove it is also an action. Certainly condition (0) is satisfied. Condition (1) is very easy since (Ha).e=H(ae)=Ha. Finally, we need to prove condition (2). Suppose that $g_{1}, g_{2} \in G$. Then

$$
\left((H a) \cdot g_{2}\right) \cdot g_{1}=\left(H\left(a g_{2}\right)\right) \cdot g_{1}=H\left(\left(a g_{2}\right) g_{1}\right)=H\left(a\left(g 2 g_{1}\right)\right)=(H a) \cdot(g 2 g 1)
$$

which proves (2) and completes the proof.
Of course, $G$ also acts on the set of left cosets of $H$ by multiplication on the left.
Example 2.5 (Another conjugation action). This example is dual to the one given above in Example 1.6. Set $G=G$ and $S=G$. Then for $g \in G$ and $x \in S$ we define $g . x=g^{-1} x g \in S=G$. I will leave it to you to verify that this is indeed a right group action.

## 3. Orbits and stabilizers

In this section we define and give examples of orbits and stabilizers. We state things for left actions first.

Definition 3.1 (Stabilizers). Suppose that $G$ acts on a set $S$ on the left. Then for $x \in S$ we define the stabilizer of $x$, denoted $\operatorname{Stab}_{G}(x)$, to be the set

$$
\operatorname{Stab}_{G}(x)=\{g \in G \mid g \cdot x=x\} .
$$

More generally, for any subset $T \subseteq S$, we can consider elements of $G$ which fix $T$.

$$
\operatorname{Fix}_{G}(T)=\{g \in G \mid g \cdot x=x \text { for all } x \in T\} .
$$

It is critical that you observe that $\operatorname{Stab}_{G}(x)$ and $\operatorname{Fix}_{G}(T)$ are subsets of $G$.
First we give a quick example:
Example 3.2. Set $G=S_{4}$ and suppose that $S=\{1,2,3,4\}$ with the group action as defined in Example 1.3. Consider the stabilizer of $2, \operatorname{Stab}_{G}(2)$. This is all the permutations $\sigma$ such that $\sigma .2=\sigma(2)=2$. For example, (13) $\in \operatorname{Stab}_{G}(2)$. In general, it is not hard to see that $\operatorname{Stab}_{G}(2)=\{e,(13),(14),(34),(134),(143)\}$. Note that $\operatorname{Stab}_{G}(2)$ is a subgroup in this case, this is not a coincidence as well shall see.
Lemma 3.3. With notation as above, both $\operatorname{Stab}_{G}(x)$ and $\operatorname{Fix}_{G}(T)$ are subgroups of $G$.
Proof. First we prove $\operatorname{Stab}_{G}(x)$ is a subgroup of $G$. Indeed, if $a, b \in \operatorname{Stab}_{G}(x)$, then we need to prove that $a b \in \operatorname{Stab}_{G}(x)$. In other words, we need to show that $(a b) . x=x$. But simply note that $(a b) \cdot x=a \cdot(b \cdot x)=a \cdot x=x$ using the fact that we have a group action and that $a$ and $b$ stabilize $x$. This proves closure for $\operatorname{Stab}_{G}(x)$. Note that $e \in \operatorname{Stab}_{G}(x)$ since $e . x=x$. Finally we need to prove inverses, so suppose that $a \in \operatorname{Stab}_{G}(x)$, we need to prove that $a^{-1} \in \operatorname{Stab}_{G}(x)$. In other words, we know $a . x=x$ and we need to show that $a^{-1} \cdot x=x$. But this is easy, simply take the equation $a . x=x$ and multiply both sides by $a^{-1}$. We get

$$
a^{-1} \cdot(a \cdot x)=a^{-1} \cdot x
$$

However, $a^{-1} \cdot(a \cdot x)=\left(a a^{-1}\right) \cdot x=e \cdot x=x$ which completes the proof that $\operatorname{Stab}_{G}(x)$ is a group.
I will leave it to you to prove that $\operatorname{Fix}_{G}(T)$ is a group, but the argument is almost exactly the same.
Remark 3.4. While $\operatorname{Stab}_{G}(x)$ is a group, it is almost never normal (unless $G$ is Abelian).
Lemma 3.5. We have an equality of sets:

$$
\operatorname{Fix}_{G}(T)=\bigcap_{x \in T} \operatorname{Stab}_{G}(x)
$$

Proof. Certainly if $g \in \operatorname{Fix}_{G}(T)$, then $g \cdot x=x$ for all $x \in T$, which proves that $g \in \operatorname{Stab}_{G}(x)$. But this proves that $g \in \bigcap_{x \in T} \operatorname{Stab}_{G}(x)$ and so we have the containment $\subseteq$. Conversely, suppose that $g \in \bigcap_{x \in T} \operatorname{Stab}_{G}(x)$. Thus $g \in \operatorname{Stab}_{G}(x)$ for all $x \in T$ and so $g \cdot x=x$ for all $x \in T$. But then $g \in \operatorname{Fix}_{G}(T)$ completing the proof.
Remark 3.6. We have so far defined stabilizers for left group actions. One can just as easily define them for right group actions and I leave it to the reader to formulate the definitions and prove the analogous properties.

While we have so far introduced stabilizers, we now introduce an equally important notion, that of the orbit.

Definition 3.7 (Orbits). Suppose that $G$ is a group acting on a set $S$ on the left. Fix $x \in S$. Then call the following set the orbit of $x$ (under $G$ )

$$
\operatorname{Orb}_{G}(x)=\{y \in S \mid y=g \cdot x \text { for some } g \in G\}=\{g \cdot x \mid g \in G\}
$$

Keep the following fact in mind.
Lemma 3.8. If $x \in S$, then $x \in \operatorname{Orb}_{G}(x)$.
Proof. $x=e . x \in \operatorname{Orb}_{G}(x)$.
We conclude our discussion with a couple more examples.
Example 3.9. We consider Example 1.4 from before. Here $G=\left\{\left.\left[\begin{array}{rr}\cos \theta & \sin \theta \\ -\sin \theta & \cos \theta\end{array}\right] \right\rvert\, \theta \in \mathbb{R}\right\}$ and $S=\mathbb{R}^{2}$ is the set of column vectors. Then for any $\mathbf{v} \in S$, it is easy to see that

$$
\operatorname{Orb}_{G}(\mathbf{v})=\left\{\mathbf{w} \in \mathbb{R}^{2}| | \mathbf{w}|=|\mathbf{v}|\}=\{\text { vectors of length }|\mathbf{v}|\} .\right.
$$

In particular, for any non-zero vector $\mathbf{v}, \operatorname{Orb}_{G}(\mathbf{v})$ is a circle of radius $|\mathbf{v}|$. On the other hand $\mathbf{v}=\mathbf{0}$, then $\operatorname{Orb}_{G}(\mathbf{v})$ is merely the origin.
Example 3.10. Consider a group $G$ acting on itself by conjugation as in Example 1.6. In other words, $G=G, S=G$, and $g \cdot x=g x g^{-1}$. Then the orbit of an element can be either just that element, or it can be many elements. I claim that the following are equivalent.
(a) $x \in Z(G)$.
(b) $\operatorname{Stab}_{G}(x)=G$
(c) $\operatorname{Orb}_{G}(x)=\{x\}$.
(d) $\left|\operatorname{Orb}_{G}(x)\right|=1$.

Let's prove this. If $x \in Z(G)$, then $x g=g x$ for all $g \in G$. Thus $x=g x g^{-1}=g . x$ for all $g \in G$. This proves that (a) implies (b) and (a) implies (c). Likewise since $x \in \operatorname{Orb}_{G}(x)$ always, (d) and (c) are clearly equivalent. On the other hand, if (c) holds, then $g \cdot x=x$ for all $g$, and so $g x g^{-1}=x$ for all $g$ and finally $g x=x g$ for all $g \in G$. This last statement proves that (c) implies (a). Finally, we need to prove that (b) implies (a). If $\operatorname{Stab}_{G}(x)=G$, then $g \cdot x=x$ for all $g \in G$ and the same logic as above implies (a) as desired.

Now we analyze the previous example in the special case of $G=S_{3}$.
Example 3.11. Consider $G=S_{3}=\{e,(12),(13),(23),(123),(132)\}$ and let it act on itself by conjugation as above. It is easy to see that $(13)(12)(13)=(23)$ and so $(23) \in \operatorname{Orb}_{S_{3}}((12))$. Then I leave it to you verify indeed that:

$$
\operatorname{Orb}_{S_{3}}((12))=\{(12),(23),(13)\}
$$

and also that

$$
\operatorname{Orb}_{S_{3}}((123))=\{(123),(132)\} .
$$

Finally, note that

$$
\operatorname{Orb}_{S_{3}}(e)=\{e\} .
$$

## 4. The orbit stabilizer theorem

In this section we prove some basic facts about orbits and stabilizers. First we prove that the orbits of a group partition the group (we didn't cover this in class on Wednesday, we'll do it on Friday).

Proposition 4.1. Suppose that a group $G$ acts on a set $S$ (on the left). Then the (distinct) orbits of $G$ partition $S$.

Proof. We need to prove two things.
(1) Every element of $S$ is in some orbit.
(2) If $\operatorname{Orb}_{G}\left(x_{1}\right) \cap \operatorname{Orb}_{G}\left(x_{2}\right) \neq \emptyset$, then $\operatorname{Orb}_{G}\left(x_{1}\right)=\operatorname{Orb}_{G}\left(x_{2}\right)$.

These two facts prove that $S$ is covered by disjoint orbits.
First we note that (1) is easy since $x \in \operatorname{Orb}_{G}(x)$ and so every element is in some orbit. Now we prove (2), suppose that $y \in \operatorname{Orb}_{G}\left(x_{1}\right) \cap \operatorname{Orb}_{G}\left(x_{2}\right)$. Thus there exists $g_{1}, g_{2} \in G$ such that $g_{1} \cdot x_{1}=y=g_{2} \cdot x_{2}$. Therefore

$$
x_{1}=e \cdot x_{1}=\left(g_{1}^{-1} g_{1}\right) \cdot x_{1}=g_{1}^{-1} \cdot\left(g_{1} \cdot x_{1}\right)=g_{1}^{-1} \cdot\left(g_{2} \cdot x_{2}\right)=\left(g_{1}^{-1} g_{2}\right) \cdot x_{2}
$$

and so $x_{1} \in \operatorname{Orb}_{G}\left(x_{2}\right)=\left\{g \cdot x_{2} \mid g \in G\right\}$. But then

$$
\operatorname{Orb}_{G}\left(x_{1}\right)=\left\{g^{\prime} \cdot x_{1} \mid g^{\prime} \in G\right\} \subseteq\left\{g^{\prime} \cdot\left(g \cdot x_{2}\right) \mid g^{\prime}, g \in G\right\} \subseteq\left\{g^{\prime} \cdot x_{2} \mid g^{\prime} \in G\right\}=\operatorname{Orb}_{G}\left(x_{2}\right)
$$

where the last containment holds because we can take $g=e$. By symmetry, we also obtain $\operatorname{Orb}_{G}\left(x_{2}\right) \subseteq \operatorname{Orb}_{G}\left(x_{1}\right)$.

Now we prove the Orbit-Stabilizer theorem.
Theorem 4.2 (Orbit Stabilizer Theorem). Suppose that $G$ is a finite group acting on a set $S$ (on the left). Then for any $x \in S$,

$$
|G|=\left|\operatorname{Orb}_{G}(x)\right| \cdot\left|\operatorname{Stab}_{G}(x)\right| .
$$

Proof. We already know that

$$
|G|=\left(\# \text { of cosets of } \operatorname{Stab}_{G}(x)\right) \cdot\left|\operatorname{Stab}_{G}(x)\right|
$$

by Lagrange's theorem. Therefore it is sufficient to prove that

$$
\left(\# \text { of cosets of } \operatorname{Stab}_{G}(x)\right)=\left|\operatorname{Orb}_{G}(x)\right| .
$$

We will give a bijection between these two sets. Define a function

$$
\Phi:\left\{\text { left cosets of } \operatorname{Stab}_{G}(x)\right\} \rightarrow \operatorname{Orb}_{G}(x)
$$

by the rule $\Phi\left(a \operatorname{Stab}_{G}(x)\right)=a . x$.
For simplicity, we write $H=\operatorname{Stab}_{G}(x)$ and so our $\Phi$ becomes $\Phi(a H)=a . x$.

We need to show that $\Phi$ is well defined, surjective, and injective. Note it is NOT a homomorphism since $\operatorname{Orb}_{G}(x)$ is almost certainly not a group.

We first show that $\Phi$ is well defined. So suppose that $a H=b H$. We need to show that

$$
\Phi(a H)=a \cdot x=b \cdot x=\Phi(b H) .
$$

Since $a H=b H$, we know that $a \in b H$ so that $a=b h$ for some $h \in H=\operatorname{Stab}_{G}(x)$. Note that $h . x=x$ by our choice of $h$. Then

$$
a \cdot x=(b h) \cdot x=b \cdot(h \cdot x)=b \cdot x
$$

which proves that $\Phi$ is well defined.
Now we prove that $\Phi$ is surjective. Suppose that $y=g . x \in \operatorname{Orb}_{G}(x)$. Then $\Phi(g H)=g . x=y$ and we conclude that $\Phi$ is surjective.

Finally, we prove that $\Phi$ is injective. Suppose that $\Phi(a H)=\Phi(b H)$. Thus $a \cdot x=b \cdot x$ and so

$$
x=e \cdot x=\left(a^{-1} a\right) \cdot x=a^{-1} \cdot(a \cdot x)=a^{-1} \cdot(b \cdot x)=\left(a^{-1} b\right) \cdot x
$$

Thus $a^{-1} b \in \operatorname{Stab}_{G}(x)=H$ by definition. Therefore $a^{-1} b H=H$ and so $b H=a H$ which proves that $\Phi$ is injective as desired.

## 5. The class equation and its corollaries

Throughout this section, we assume the following notation, that $G$ is a group acting on $S=G$ by conjugation as in Example 1.6. In other words, for $g \in G$ and $x \in S=G$, we define $g . x=g x g^{-1}$. Our main goal in the section is:
Theorem 5.1 (The Class Equation). Suppose that a finite group $G$ acts on itself by conjugation, then

$$
|G|=|Z(G)|+\sum_{x \text { in disjoint nontrivial orbits }}|G| /\left|\operatorname{Stab}_{G}(x)\right|
$$

Proof. We know

$$
G=\bigcup_{x \text { in disjoint orbits }} \operatorname{Orb}_{G}(x)
$$

from Proposition 4.1. An element $x \in S=G$ has trivial orbit (equal to $\{x\}$ ) if and only if $x \in Z(G)$ by Example 3.10.

Thus we know that $G$ is also the disjoint union

$$
G=(Z(G)) \bigcup\left(\bigcup_{x \text { in disjoint orbits }} \operatorname{Orb}_{G}(x)\right)
$$

Since this is a disjoint union, we have

$$
|G|=|Z(G)|+\sum_{x \text { in disjoint nontrivial orbits }}\left|\operatorname{Orb}_{G}(x)\right| .
$$

Finally, using the Orbit Stabilizer Theorem, Theorem 4.2, we have:

$$
|G|=|Z(G)|+\sum_{x \text { in disjoint nontrivial orbits }}|G| /\left|\operatorname{Stab}_{G}(x)\right| .
$$

Now we prove Cauchy's theorem.
Theorem 5.2 (Cauchy's Theorem). Suppose that $G$ is a group and that a prime $p$ divides the order of $G$. Then $G$ contains an element of order $p$.

Proof. We proceed by strong induction on $n=|G|$. In particular, we assume that the theorem holds for all groups of size less than $n=|G|$.

If $G$ is Abelian, then we already know the theorem since we proved it earlier. Therefore, we may assume that $G$ is not Abelian, in particular $Z(G) \neq G$. We again view $G$ acting on itself by conjugation.

Suppose by way of contradiction, that $G$ does not contain an element of order $p$. It follows then that neither does $Z(G)$ (since $Z(G)$ is a subgroup of $G$ ) and neither does $\operatorname{Stab}_{G}(x)$ for any $x$ (since they are also subgroups of $G$ ). In particular, by our inductive hypothesis, we may assume that $p$ does not divide the order of $Z(G)$ or the order of any $\operatorname{Stab}_{G}(x)$.

Now we apply the Class Equation:

$$
|G|-\sum_{x \text { in disjoint nontrivial orbits }}|G| / / \operatorname{Stab}_{G}(x)|=|Z(G)|
$$

Since $p$ divides $|G|$ and does not divide $\left|\operatorname{Stab}_{G}(x)\right|$, we have that $p$ divides $|G| /\left|\operatorname{Stab}_{G}(x)\right|$. Thus $p$ divides the left side of the equation. But $p$ does not divide the right side of the equation and so we have an contradiction. Thus $G$ must contain an element of order $p$.

Here's another simple corollary of the Class Equation.
Corollary 5.3. Suppose that $G$ is a finite group of order $p^{n}$ where $p$ is a prime. Then $Z(G) \neq\{e\}$.
Proof. When we apply the Class Equation again, we get

$$
|G|-\sum_{x \text { in disjoint nontrivial orbits }}|G| /\left|\operatorname{Stab}_{G}(x)\right|=|Z(G)|
$$

Now, $p$ divides $|G|$, and since we are summing over nontrivial orbits, $p$ divides each $|G| /\left|\operatorname{Stab}_{G}(x)\right|$. Thus $p$ divides $|Z(G)|$ as well, and so $|Z(G)| \neq 1$.

Finally, we prove a short corollary of the previous corollary.
Corollary 5.4. If $G$ is a finite group of order $p^{2}$ where $p$ is prime, then $G$ is Abelian.
Proof. We know $Z(G) \neq\{e\}$ by Corollary 5.3. Thus $|Z(G)|$ is either $p$ or $p^{2}$. If $|Z(G)|=p^{2}$, then $Z(G)=G$ and so $G$ is Abelian. Thus we may assume that $|Z(G)|=p$ and so $|G / Z(G)|=$ $|G| /|Z(G)|=p^{2} / p=p$. Therefore $G / Z(G)$ is a group of order $p$, and so it is cyclic. By one of the problems on the exam, we see that $G$ is Abelian, which completes the proof.

