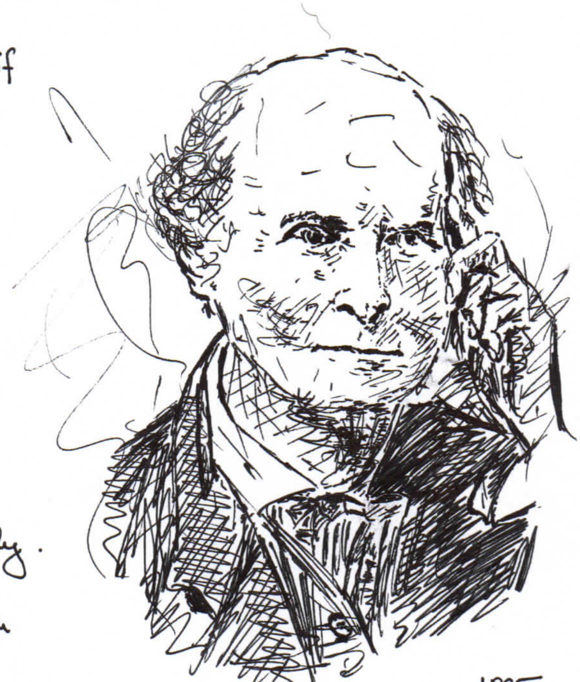
2 GROUPS ACTING ON SETS, CAYLEY'S THEOREM, BURNSIDE'S THEOREM



Arthur Cayley 1821 – 1895

Definition: A group G acts (on the left) on a set X if for each $g \in G$ and each $x \in X$ there is an element $gx \in X$ such that

1) $g(hx) = (gh).x$ for all $g, h \in G$, $x \in X$

2) $1 \cdot x = x$ for all $x \in X$.

We can define a group G acting on the right on X similarly. In this case we have for each $g \in G$ and each $x \in X$ an element $xg \in X$ such that

1') $(xh)g = x(hg)$ for all $g, h \in G$, $x \in X$

2') $x1 = x$ for all $x \in X$.

To a given left action of G on a set X corresponds a right action defined by $x \cdot g := g^{-1}x$, for all $g \in G$, $x \in X$.

Given a set X let $S(X)$ denote the group of all bijections $X \to X$. The group $S(X)$ will be called the symmetric group of X. Then left actions of a group G on a set X are exactly homomorphisms of the group G to $S(X)$.

- The kernel of an action of G on X on the left is the kernel of the corresponding homomorphism. It is the normal subgroup

$$K := \{ g \in G \mid gx = x \text{ for every } x \in X \}$$

CAYLEY'S THEOREM:

Theorem 2.1 (Cayley): Let H be a subgroup of a group G, let X denote the set of all left cosets of H in G.

- The group G acts on the set X on the left by left multiplication, i.e., $g \cdot (h \cdot H) = (gh) \cdot H$ for all $g \in G$ and all $hH \in X$.
- The kernel of this action is

$$K = \bigcap_{g \in G} gHg^{-1}.$$

Proof: That the left multiplication induces a left action on the set X is straightforward:

- $g_2(g_1 \cdot \ell H) = g_2 g_1 \ell H = (g_2 g_1) \cdot \ell H$ for all $g_1, g_2, \ell \in H$,
- $1 \cdot \ell H = \ell H$ for all $\ell \in H$.

For $g, k \in G$:

$k \cdot gH = gH$ iff $g^{-1}kgH = H$ iff $g^{-1}kg \in H$ iff $k \in gHg^{-1}$.

Therefore the kernel of the left action is the intersection of all the sets gHg^{-1}! $\square$

Corollary 2.2: Let H be a subgroup of G and X denote the set of all left cosets of H in G.

Define a mapping
$$\phi : G \longrightarrow S(X)$$
$$g \longmapsto \left[\begin{array}{l}\phi_g : X \to X \\ \quad \ell H \mapsto g\ell H\end{array}\right].$$

Then ϕ is a homomorphism with kernel $\bigcap_{g\in G} gHg^{-1}$.

Proof. ϕ is the homomorphism corresponding to the left action by the left multiplication of G on X. $\square$

Definition: For $H = \{1\}$, the homomorphism $\phi : G \to S(X)$ from the previous Corollary is called <u>the (left) regular representation</u> of the group G.

Proposition 2.3: Let G be a group.

1. The (left) regular representation of the group G is an embedding of the group G into the group $S(G)$.
2. The image of a non-trivial element $g \in G$ is a permutation ϕ_g which sends

Proof. 1. The left cosets of $\{1\}$ in G are of size 1, and so they can be identified with elements of G. Thus $\phi : G \to S(G)$ is a homomorphism with $\operatorname{Ker}\phi = \bigcap_{g\in G} \underbrace{g\{1\}g^{-1}}_{=\{1\}} = \{1\}$. We see that ϕ is an embedding.

2. For $g \in G$ and $x \in G$: $x = \phi_g(x) = gx$ iff $1 = g$. $\square$

Corollary 2.4: A finite group G can be embedded into S_n where $n = |G|$.

Corollary 2.5: Given a field $\mathbb{F}$ and a finite group G, there is an embedding $G \hookrightarrow GL_n(\mathbb{F})$, where $n = |G|$.

Proof. There is an embedding $S_n \to GL_n(\mathbb{F})$; $a_{ij} = \begin{cases} 1 & \text{if } \pi(j) = i \\ 0 & \text{otherwise.} \end{cases}$ $\square$

$\pi \mapsto A_\pi = (a_{ij})$

Exercise: Verify that $A_\sigma A_\pi = A_{\sigma\circ\pi}$ for all $\pi, \sigma \in S_n$.

Proposition (Poincaré) 2.6. Let H be a subgroup of a group G of a finite index m. Then H contains a subgroup N such that

- N is a normal subgroup of G of a finite index, say k, in G
- $m \mid k$ and $k \mid m!$

Proof: Let X denote the set of all left cosets of H in G. Let $\phi : G \to S(X)$ be the homomomorphism induced by the left caction of G on X by left multiplication (as in the Cayley's theorem).

Put $N = \operatorname{Ker}\phi$. Since $G/_{\operatorname{Ker}\phi} \simeq \operatorname{Im}\phi$, the index of N in G equals the size of $\operatorname{Im}\phi$. Since $|X| = m$, $\operatorname{Im}\phi$ is isomorphic to a subgroup of S_m, hence $k \mid m!$. Finally, since $\ker\phi \le H \le G$, note that $\ker\phi = \bigcap_{g\in G} gHg^{-1} \le H$, $m \mid k$. $\square$

Burnside's theorem

William Burnside 1839 – 1920

Let a group G acts on the left on a set X.

- An **orbit** of an element $x \in X$ is the set

$$Gx := \{gx \mid g \in G\}$$

Define a binary relation $\sim_G$ on the set X by $x \sim_G y$ if $x = gy$ for some $g \in G$. It is easy to observe that $\sim_G$ is an equivalence:

- reflexivity: $x = 1x$ so $x \sim_G x$
- transitivity: If $x \sim_G y \sim_G z$, there are $g, h \in G$ such that $x = gy$ and $y = hz$. Then $x = g(hz) = (gh)\cdot z$, and so $x \sim_G z$
- symmetry: $x \sim_G y$, then $x = gy$ for some $g \in G$ and $y = g^{-1}x$, hence $y \sim_G x$.

It follows from the definition, that orbits are blocks of the equivalence relation $\sim_G$. In particular, orbits form a partition of the set X. They do not need to be of the same size!

Example: Consider the action of a group G on the set G by conjugation. That is

$$g\cdot x = gxg^{-1}$$

for all $\underbrace{g \in G}_{\text{the group}}$, $\underbrace{x \in G}_{\text{the set}}$. It is straigforward to verify that this is a left action.

For $G = S_3$ we have the following orbits: $\{1\}$, $\{(12),(13),(23)\}$, $\{(123),(132)\}$.

- The stabiliser of an element $x \in X$ is

$$St_G(x) := \{ g \in G \mid g\cdot x = x \}.$$

Lemma 2.7: Let a group G acts on the left on a set X. For every $x \in X$:

- $St_G(x)$ is a subgroup of the group G.
- $|Gx| = |G : St_G(x)|$
- Stabilisers of elements from the same orbit are conjugated.

Proof:
- If $g, h \in St_G(x)$, then $(h^{-1}g)\cdot x = h^{-1}(gx) = h^{-1}x = h^{-1}(hx) = 1\cdot x = x$, hence $St_G(x)$ is a subgroup of G.
- Let X denote the set of all left cosets of $St_G(x)$ in G. Define a map

$$\begin{aligned} Gx &\longrightarrow X \\ gx &\longmapsto g\cdot St_G(x) \end{aligned}$$

Since $gx = hx$ iff $(h^{-1}g)x = x$ iff $h^{-1}g \in St_G(x)$ iff $g\,St_G(x) = h\,St_G(x)$, the map is well defined and one-to-one. It is clearly onto, therefore it is a bijection.

- Let x, hx are elements from the same orbit ($x \in X, h \in G$). Then

$$g \in St_G(h\cdot x) \text{ iff } ghx = hx \text{ iff } h^{-1}ghx = x \text{ iff } h^{-1}gh \in St_G(x)$$

Therefore $St_G(h\cdot x) = h^{-1}\,St_G(x)\,h$. $\square$

- The fixed points set of an element $g \in G$ is

$$Fix(g) = \{ x \in X \mid gx = x \}$$

- Given a left action of a group G on a set X, let

$$X/G := \{ Gx \mid x \in X \}$$

denote the set of all orbits.

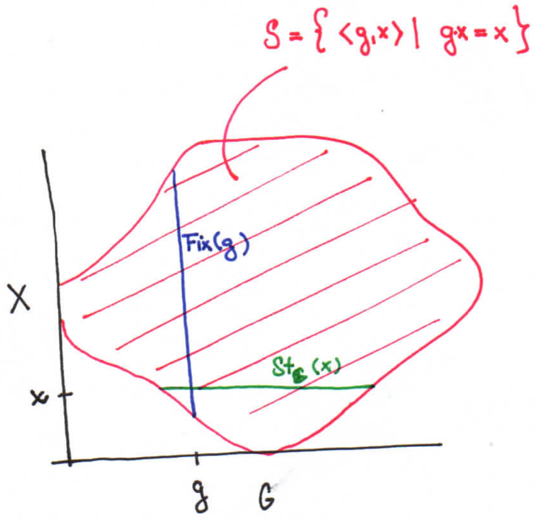
$$|X/G| = |\{Gx \mid x \in X\}| = \sum_{Gx \in X/G} 1 = \sum_{Gx \in X/G} \left(\frac{1}{|Gx|} \sum_{y \in Gx} 1 \right) = \sum_{Gx \in X/G} \sum_{y \in Gx} \frac{1}{|Gx|} = \sum_{x \in X} \frac{1}{|Gx|}$$

This formula allows us to count the number of orbits as

$$|X/G| = \sum_{x \in X} \frac{1}{|Gx|} \qquad (1)$$

Theorem (Burnside) 2.8: Let a group G acts on a left on a set X. Then

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| .$$



Proof. Put

$$S = \{ \langle g,x \rangle \mid g \cdot x = x \} .$$

The horizontal fibers of the set S are sets ~~Fix~~ $St_G(x)$, $x \in X$, while vertical fibers are the sets $\mathrm{Fix}(g)$, $g \in G$. We can count the size of the set S in two ways:

$$|S| = \sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} |St_G(x)| \qquad (2)$$

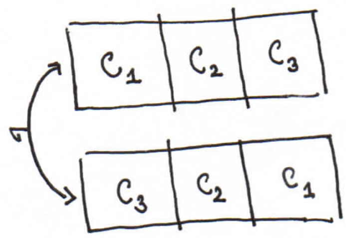
By the previous lemma, $|G| = |G : St_G(x)| \cdot |St_G(x)| = \cancel{|G : St_G(x)|}\, |Gx| \cdot |St_G(x)|$, hence $|St_G(x)| = \frac{|G|}{|Gx|}$. Applying (1), we get that

$$|X/G| = \sum_{x \in X} \frac{1}{|Gx|} = \frac{1}{|G|} \sum_{x \in X} \frac{|G|}{|Gx|} = \frac{1}{|G|} \sum_{x \in X} |St_G(x)| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| .$$

□

Example: Consider the following proplem: Consider we have 9 colors.

- How many striped flags are there having 3 stripes? (We assume all strips have the same size and are vertical).



Solution. When we ~~put~~ turn the flag upside-down we get another flag. Let $\sigma \in S_3$ be the transposition $(1,3)$ corresponding to "turning the flags". Then the subgroup $\langle \sigma \rangle \leq S_3$ acts on the set X of "drawn flags on the paper" and the number of different flags is the number of orbits. By Burnsides lemma:

$$\underbrace{|X/G|}_{\text{the number of flags}} = \underbrace{\frac{1}{2}}_{\text{the size of } \langle \sigma \rangle} \Big(\underbrace{9^3}_{|\mathrm{Fix}(1)|} + \underbrace{9^2}_{|\mathrm{Fix}(\sigma)|} \Big)$$

(Observe that σ sigma fix exactly flags with the first and the third strip of the same color).

- If we replace 3 by n, we get

$$|X/G| = \frac{1}{2}\left(9^n + 9^{\left[\frac{n+1}{2}\right]} \right),$$ where $[k]$ is the least integer bigger or equal k.

□

PÓLYA'S THEOREM

- For $n \in \mathbb{N}$ put $\hat{n} = \{1, 2, \dots, n\}$.

George Pólya
1887 – 1985

Definition: Let C be a set (of colors). The symmetric group S_n acts on the set C^n (of n-tuples of colors) by

$$\gamma \cdot \langle c_1, \dots, c_n \rangle = \langle c_{\gamma(1)}, \dots, c_{\gamma(n)} \rangle$$

for $\gamma \in S_n$. If $G \leq S_n$ and $|C| = q$ we call an orbit of C^n by $\langle q, G \rangle$-coloring of $\hat{n}$.

⚠ Let C be a set of colors and $\gamma \in S_n$. Then an n-tuple $\langle c_1, \dots, c_n \rangle$ belongs to $\mathrm{Fix}(\gamma)$ iff all elements in every cycle of γ have the same color.

- For $\gamma \in S_n$, let $c(\gamma)$ denote the number of cycles of γ (including cycles of length 1).

For example, for $\gamma = (12)(456) \in S_6$, $c(\gamma) = 3$.

Lemma 2.9: Let C be a set of colors of size q, let $G \leq S_n$. For $\gamma \in G$:

$$|\mathrm{Fix}(\gamma)| = q^{c(\gamma)}.$$

- Let $\gamma \in S_n$. For $i \in \{1, \dots, n\}$, let $c_i(\gamma)$ denote the number of cycles of length i in the complete factorization o γ into a product of independent cycles. The index of γ is

$$i(\gamma) = x_1^{c_1(\gamma)} x_2^{c_2(\gamma)} \cdots x_n^{c_n(\gamma)}$$

- Let $G \leq S_n$. The cycle index of G is the polynomial

$$P_G(x_1, \dots, x_n) = \frac{1}{|G|} \sum_{\gamma \in G} i(\gamma) \quad \in \mathbb{Q}[x_1, \dots, x_n].$$

Proposition 2.10: Let $G \leq S_n$. The number of $\langle q, G \rangle$-colorings of $\hat{n}$ is $P_G(q, \dots, q)$.

Proof. For $\gamma \in G$, $c(\gamma) = \sum_{i=1}^{n} c_i(\gamma)$ and so

$$|\mathrm{Fix}(\gamma)| = q^{c(\gamma)} = i(\gamma)(q, \dots, q)$$

Now, apply Burnside's theorem.

□

Theorem (Pólya 1937) 2.11 Let $G \le S_n$ and let $C = \{c_1, \dots, c_q\}$ be a set of q "colors".
For each $i \in \{1, \dots, n\}$ let
$$\sigma_i = \sum_{j=1}^{q} c_j^i .$$
Then the number of $\langle q, G\rangle$-colorings of $\hat{n}$ with exactly k_i-elements of color c_i is the coeficient of $c_1^{k_1} c_2^{k_2} \dots c_q^{k_q}$ in the polynomial $P_G(\sigma_1, \dots, \sigma_n)$.

TRANSITIVITY

Definition: Let a group G acts on the left on a set X.

- Say that G acts on X *faithfully* if it has a trivial kernel, i.e., if for every $1 \ne g \in G$ there exists $x \in X$ such that $g \cdot x \ne x$.
- We say that G acts on X *k-transitively* if for any $\langle x_1, \dots, x_k\rangle, \langle y_1, \dots, y_k\rangle \in X^k$ such that $x_i \ne x_j$ and $y_i \ne y_j$ for $i \ne j$, there is $g \in G$ s.t. $g \cdot x_i = y_i$ for all $i \in \{1, \dots, k\}$.

- The group S_n acts on $\{1, \dots, n\}$ n-transitively.
- The group A_n acts on $\{1, \dots, n\}$ $(n-2)$-transitively.

Proposition. 2.12 If a group G acts on a set X faithfully and 2-transitively, then every non-trivial normal subgroup acts on X transitively.

Proof. Let $1 < H \trianglelefteq G$. Assume that H does not act on X transitively. Then there are at least two orbits $Hx_1 \ne Hx_2$. Since G acts on X faithfully and H is non-trivial, at least one of the orbits has more than one-element; say $|Hx_1| > 1$, hence there is $h \in H$ s.t. $hx_1 \ne x_1$. Since G acts on X transitively, there is $g \in G$ s.t. $g\cdot\{x_1\} = x_2$ and $g\{h\cdot x_1\} = x_1$.
Then $ghg^{-1} \cdot x_2 = gh \cdot x_1 = g \cdot hx_1 = x_1$. But then $x_1 \in Hx_2$ ↯. □

$$\begin{tikzcd} x_1 \arrow[r, mapsto, "h"] \arrow[d, "g"'] & hx_1 \arrow[d, "g"] \\ x_2 & x_1 \end{tikzcd}$$

- Let G acts on a set X and $H \le G$. The sets
$Hx = \{h \cdot x \mid h \in H\}$, $x \in X$ are called *H-orbits*.

Suppose that $H \trianglelefteq G$. Then G acts on the set of all H-orbits via
$$g \cdot (Hx) = gH \cdot x = H \cdot (g \cdot x)$$

Proposition: 2.13 Suppose that a group G acts transitively on a set X and let $H \trianglelefteq G$. Then

- G acts transitively on the set of H-orbits
- All H-orbits have the same size.

Proof. • Let Hx, Hy be H-orbits. Since G acts on X transitively, there is $g \in G$ s.t. $gx = y$. Then $g \cdot Hx = Hgx = Hy$.

since $H \trianglelefteq G$

• Define a map
$$\phi : Hx \longrightarrow Hy$$
$$h \cdot x \mapsto (g \cdot h g^{-1}) \cdot y$$

It is easy to see that ϕ is a bijection with an inverse map
$$\psi : Hy \longrightarrow Hx$$
$$h \cdot y \longmapsto (g^{-1} h g) x$$

In particular, the map ϕ is well defined as $hx = h'x \Rightarrow ghg^{-1}y = ghx = gh'x = gh'g^{-1}y$, and so $hx = h'x \Rightarrow \phi(hx) = \phi(h'x)$. $\square$

CENTER OF A GROUP, NORMALIZERS AND CENTRALIZERS

• The center of a group G is
$$Z(G) := \{ g \in G \mid \forall h \in G : gh = hg \}$$

Observe that $Z(G)$ is the kernel of the left action of G on G by conjugation. Indeed, $Z(G) = \{ g \in G \mid \forall h \in G : ghg^{-1} = h \}$. It follows that $Z(G)$ is a normal subgroup of the group G.

Definition. Let p be a prime. A p-group is a group in which every element has order a power of p.

Lemma 2.14: Let A be a finite abelian group. If a prime p divides the order of A, then A contains an element of order p.

Proof: • First assume that $A = \langle a \rangle$ is a cyclic group. Then $o(a) = |A| = p \cdot m$ for some $m \in \mathbb{N}$. Then $b = a^m$ is an element of order p.

• In the general case, let $|A| = p \cdot m$. We will proceed by induction on m. Pick a non-trivial element $a \in A$. If $p \mid o(a)$, there is an element of order p in the cyclic group $\langle a \rangle$. Suppose that $p \nmid o(a)$. Then $A/\langle a \rangle$ is a smaller abelian group. By Lagrange theorem $p \mid |A/\langle a \rangle|$. By the induction hypothesis, there is an element $b \cdot \langle a \rangle$ of order p. Therefore $p = \langle a, b \rangle / \langle a \rangle$ and since
$$\langle a, b \rangle / \langle a \rangle \simeq \langle b \rangle / \langle a \rangle \cap \langle b \rangle$$
and by the Lagrange theorem
$$|\langle b \rangle| = \left| \langle b \rangle / \langle a \rangle \cap \langle b \rangle \right| \cdot \left| \langle a \rangle \cap \langle b \rangle \right|,$$
$p \mid |\langle b \rangle|$. We conclude that $\langle b \rangle$ contains an element of order p. $\square$

Definition. Let $H \leq G$, let $a \in G$:

- The normaliser of the subgroup H in the group G is

$$N_G(H) := \{ g \in G \mid gHg^{-1} = H \}.$$

- The centraliser of the element a in G is

$$C_G(a) := \{ g \in G \mid gag^{-1} = a \}.$$

Lemma 2.15: Let $H \leq G$ and $a \in G$. Then

1) $N_G(H) \leq G$, $C_G(H) \leq G$;

2) $H \trianglelefteq N_G(H)$ and $\langle a \rangle \leq Z(C_G(a))$.

Proof: 1) • Let $g, h \in N_G(H)$. Then

- $g^{-1}Hg = g^{-1}(gHg^{-1})g = H$, hence $g^{-1} \in N_G(H)$.
- $(gh)H(gh)^{-1} = ghHh^{-1}g^{-1} = gHg^{-1} = H$, hence $gh \in N_G(H)$.

Therefore $N_G(H)$ is a subgroup of G.

• Let $g, h \in C_G(a)$. Then

- $g^{-1}ag = g^{-1}(gag^{-1})g = a$, hence $g^{-1} \in C_G(a)$.
- $(gh)a(gh)^{-1} = ghah^{-1}g^{-1} = gag^{-1} = a$, hence $gh \in C_G(a)$.

Therefore $C_G(a)$ is a subgroup of G.

2) Follows readily from the definitions of $N_G(H)$ and $C_G(a)$. $\square$

Remark: Informally, $N_G(H)$ is ~~the~~ a largest subgroup of G in which H is normal and $C_G(a)$ is a largest subgroup of G such that a is in its center.

Lemma 2.16: 1) Let H be a subgroup of a group G. Then

$$|\{ gHg^{-1} \mid g \in G \}| = |G : N_G(H)|.$$

2) Let $a \in G$. Then

$$|\{ gag^{-1} \mid g \in G \}| = |G : C_G(a)|.$$

Proof. 1) Put $M := \{ gHg^{-1} \mid g \in G \}$; the set of all subgroups of G conjugated with H in G. The group G acts on the set M by conjugation: $g \cdot (xHx^{-1}) = gxHx^{-1}g^{-1} = (gx)H(gx)^{-1}$. This action is transitive, and so the orbit $G \cdot H$ of H is the set M. Observe that $St_G(H) = N_G(H)$. Therefore $|G \cdot H| = |M| = |G : St_G(H)| = |G : N_G(H)|$.

2) The group G acts on the set G by conjugation, i.e., $g\cdot x = gxg^{-1}$ for all $x, g \in G$.
Observing that $G\cdot a = \{g^{-1}ag \mid g \in G\}$ and $St_G(a) = C_G(a)$, we get that

$$|\{gag^{-1} \mid g \in G\}| = |G\cdot a| = |G : St_G(a)| = |G : C_G(a)|.$$

□

As above, consider the left action of a group G on the set G by conjugation. For every $g \in G$, $C_G(g) = St_G(g)$ and $Z(G)$ is the set of all $g \in G$ whose stabilizer is the whole G. We can also view $Z(G)$ as the set of those $g \in G$ whose orbit is a single element, the g. Let Δ be some set of representatives of orbits that have at least two elements. Since the group G is a disjoint union of orbits, we get that

$$|G| = |Z(G)| + \sum_{g\in\Delta} |G : C_G(g)| \qquad (*)$$

Definition: Equation $(*)$ above is called the <u>class formula</u> for a finite group G.

Theorem (Cauchy) 2.17. Let G be a finite group. If $p \mid |G|$ for a prime p, then G contains an element of order p.

Proof. We proceed by induction on the size of G. Again, as above, consider the left action of the group G on G by conjugation. Observe that if $g \notin Z(G)$, then $C_G(g)$ is a proper subgroup of G. If $p \mid |C_G(g)|$ for such a g, then $C_G(g)$ would contain an element of order p by the induction hypothesis. Therefore $p \nmid |C_G(g)|$ and from the Lagranges theorem we get that

$$|G| = |G : C_G(g)| \cdot |C_G(g)|.$$

Since p is a prime, $p \mid |G : C_G(g)|$. Let Δ be a set of representatives of orbits with at least two elements. By the class formula

$$|Z(G)| = |G| - \sum_{g\in\Delta} |G : C_G(g)|.$$

Since the right hand side of the equation is divisible by p, $p \mid |Z(G)|$. Therefore $Z(G)$ is an abelian group of order divisible by p, hence it contains an element of order p, by a lemma above.

□

Lemma 2.18: A finite group G is a p-group iff $|G| = p^k$.

Proof: ($\Leftarrow$) The order of an element of a finite group divides the order of the group (by the Lagrange's theorem). Therefore, if $|G| = p^k$, the order of every $g \in G$ is a power of p, and so G is a p-group.

($\Rightarrow$) If $|G|$ is not a power of p, there is a prime $q \neq p$ such that $q \mid |G|$. By the Cauchy's theorem, there is an element of order q in G. It follows that G is not a p-group. $\square$

Theorem 2.19: The center of a finite p-group is non-trivial.

Proof: Let once again act G on G by conjugation. As above, let Δ denote the set of representatives of orbits with at least two elements. Since G is a p-group $|G : C_G(g)|$ is a positive power of p for every $g \in \Delta$. Applying the class formula, we get that

$$|Z(G)| = |G| - \sum_{g \in \Delta} |G : C_G(g)|.$$

As $p \mid |G : C_G(g)|$ for all $g \in \Delta$, p divides the right hand side of the equation. Therefore $p \mid |Z(G)|$, in particular, the center $Z(G)$ is non-trivial. $\square$