11-11-1993

Group actions.

Definition. Let G be a group, and let X be a set. An **action** (more properly, a **left action**) of G on X is a function $\theta : G \times X \to X$ satisfying:

1. $\theta(g_1, \theta(g_2, x) = \theta(g_1 g_2, x)$ for all $g_1, g_2 \in G$ and $x \in X$.
2. $\theta(1, x) = x$ for all $x \in X$.

   It's customary to write "$g \cdot x$" or "gx" for $\theta(g, x)$; the equations above then become

$$g_1(g_2 x) = (g_1 g_2)x \quad \text{and} \quad 1 \cdot x = x.$$

   If G acts on X, X is a G-**set**.

Lemma. If X is a G-set, there is a homomorphism $\phi : G \to S_X$, where S_X is the group of permutations of X. Conversely, any homomorphism $\phi : G \to S_X$ gives rise to a G-set structure on X.

Proof. Let X be a G-set. Define $\phi : G \to S_X$ by

$$\phi(g)(x) = gx.$$

Since $\phi(g^{-1})\phi(g)(x) = x$ and $\phi(g)\phi(g^{-1})(x) = x$, $\phi(g)$ and $\phi(g^{-1})$ are inverses. Therefore, $\phi(g)$ is a bijection, so $\phi(g) \in S_X$.

To see that ϕ is a homomorphism, note that

$$\phi(g_1)\phi(g_2)(x) = g_1(g_2 x) = (g_1 g_2)x = \phi(g_1 g_2)(x).$$

Conversely, suppose $\phi : G \to S_X$ is a homomorphism. Define an action of G on X by

$$g \cdot x = \phi(g)(x).$$

Then

$$\phi(g_1 g_2)(x) = \phi(g_1)\phi(g_2)(x) \quad \text{so} \quad (g_1 g_2)x = g_1(g_2 x).$$

This verifies property 1.

Since ϕ is a homomorphism, $\phi(1) = \text{id}$. Hence, $1 \cdot x = \phi(1)(x) = \text{id}(x) = x$. This verifies property 2. Hence, X is a G-set. $\square$

Examples. 0. Any group G acts on any set X by defining $g \cdot x = x$ for all $g \in G$ and all $x \in X$. $\square$

1. Let $\mathbb{Z}$ act on $\mathbb{R}$ by translation. That is, if $n \in \mathbb{Z}$ and $x \in \mathbb{R}$, define $n \cdot x = x + n$. Now

$$n_1 \cdot (n_2 \cdot x) = n_1 \cdot (x + n_2) = x + n_2 + n_1 = (n_1 + n_2) \cdot x$$

$$0 \cdot x = x + 0 = x$$

Therefore, this is an action of $\mathbb{Z}$ on $\mathbb{R}$. $\square$

2. Let

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}.$$

Make G into a group via matrix multiplication. G acts on $\mathbb{R}^2$ by multiplication: e.g.

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}.$$

Notice that

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{fixes everything}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{fixes } y = 0 \text{ (the } x\text{-axis)}$$

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{fixes } x = 0 \text{ (the } y\text{-axis)}$$

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{fixes the origin. } \square$$

3. S_3 acts on $\{1, 2, 3\}$. And in general, S_n acts on $\{1, 2, \ldots, n\}$. $\square$

Definition. Let X be a G-set, and let $x \in X$. The **orbit** of x under the action is

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

The set of orbits of X under G is denoted X/G.

If $X = Gx$ for some $x \in X$, the action is **transitive**. (In this case, X is said to be a **transitive** G**-set**.)

Lemma. X is a transitive G-set if and only if for all $x, y \in X$, there exists $g \in G$ such that $gx = y$.

Proof. ($\Rightarrow$) Since X is transitive, $X = Gz$ for some $z \in X$. Let $x = g_1 z$ and let $y = g_2 z$, where $g_1, g_2 \in G$. Then $g_1^{-1} x = z$, so $y = g_2 g_1^{-1} x$.

($\Leftarrow$) Suppose that for all $x, y \in X$, there exists $g \in G$ such that $gx = y$. Take any $x \in X$. If $y \in X$, then $gx = y$ for some $g \in G$, so $y \in Gx$. Thus, $X \subset Gx$, so $X = Gx$, and X is a transitive G-set. $\square$

Definition. Let X be a G-set, and let $x \in X$. The **isotropy group** of x is

$$G_x = \{g \in G \mid gx = x\}.$$

If $G_x = \{1\}$ for all $x \in X$, the action is **free**. (In this case, X is called a **free** G**-set**.)

Example. Let D_3, the dihedral group of order 6, act on the vertices $\{1, 2, 3\}$ of an equilateral triangle. If m_1 denotes reflection through the line through vertex 1, then the isotropy group of vertex 1 is $\{\mathrm{id}, m_1\}$ (and similarly for the other two vertices). $\square$

Lemma. Let X be a G-set, and let $x \in X$. Then $G_x < G$.

Proof. First, $1 \cdot x = x$, so $1 \in G_x$. Suppose $g \in G_x$. Then $gx = x$, so $x = g^{-1}x$. Therefore, $g^{-1} \in G_x$.

Finally, suppose $g, h \in G_x$. Then

$$(gh)x = g(hx) = gx = x.$$

Hence, $gh \in G_x$. Therefore, $G_x < G$. $\square$

Examples. 1. Consider the translation action of $\mathbb{Z}$ on $\mathbb{R}$ defined above. An orbit has the form

$$x + \mathbb{Z} = \{x + n \mid n \in \mathbb{Z}\}, \quad \text{where} \quad 0 \le x < 1.$$

Thus, the space of orbits $\mathbb{R}/\mathbb{Z}$ is equivalent to S^1, the circle. (Of course, the two are actually isomorphic as groups!)

The action is free, since the only $n \in \mathbb{Z}$ which fixes $x \in \mathbb{R}$ is 0. On the other hand, the action is not transitive: There is no integer translation carrying 0 to $\dfrac{1}{2}$, for instance. $\square$

2. Consider the action of the group

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

on the plane $\mathbb{R}^2$.

The isotropy groups of points under this action are:

$$G_{(0,0)} = G$$

$$G_{(x,0)} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\} \text{ for } x \neq 0$$

$$G_{(0,y)} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \right\} \text{ for } y \neq 0$$

$$G_{(x,y)} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \text{ for } x, y \neq 0$$

Obviously, the action is not free.

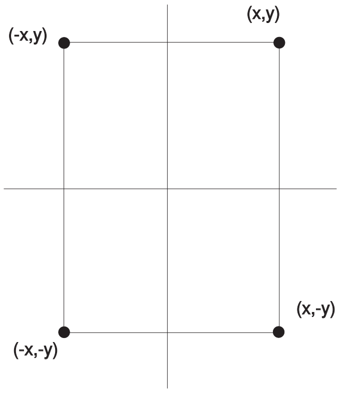
The orbits of points under the action are:

$$\{(0,0)\}$$

$$\{(x,0), (-x,0)\} \text{ for } x \neq 0$$

$$\{(0,y), (0,-y)\} \text{ for } y \neq 0$$

$$\{(x,y), (-x,y), (x,-y), (-x,-y)\} \text{ for } x, y \neq 0$$



Since there is more than one orbit, the action is not transitive.

The set of orbits $\mathbb{R}^2/G$ looks like the first quadrant $\{(x,y) \mid x, y \geq 0\}$. $\square$

3. Consider the action of S_3 on $\{1,2,3\}$. The action is transitive: If $i, j \in \{1,2,3\}$, $i \neq j$, the transposition (ij) carries i to j. (If $i = j$, there's nothing to do.)

The isotropy groups are

$$G_{\{1\}} = \{\mathrm{id}, (2\ 3)\}$$

$$G_{\{2\}} = \{\mathrm{id}, (1\ 3)\}$$

$$G_{\{3\}} = \{\mathrm{id}, (1\ 2)\} \ \square$$

Proposition. Let X be a G-set. Then X is partitioned by the orbits.

Proof. If $x \in X$, then $x \in Gx$. Hence, X is certainly the union of the orbits. I need to show that two orbits are either disjoint or identical.

Suppose that $Gx \cap Gy \neq \emptyset$. Find $z \in Gx \cap Gy$. Then $z = g_1 x$ and $z = g_2 y$ for some $g_1, g_2 \in G$. Hence, $g_1 x = g_2 y$, so $x = g_1^{-1} g_2 y$ and $y = g_2^{-1} g_1 x$.

Now let $gx \in Gx$. Then $gx = g g_1^{-1} g_2 y \in Gy$. This proves $Gx \subset Gy$. Likewise, if $gy \in Gy$, then $gy = g g_2^{-1} g_1 x \in Gx$, so $Gy \subset Gx$. Therefore, $Gx = Gy$. Hence, two orbits which intersect nontrivially must in fact coincide. This proves that the orbits partition X. □

There is a group-theoretic relationship between isotropy groups of points in the same orbit.

Proposition. Let X be a G-set, let $x \in X$, and let $g \in G$. Then

$$G_{gx} = g G_x g^{-1}.$$

Proof. Suppose $h \in G_{gx}$, so $hgx = gx$. Then $g^{-1} h g x = x$, so $g^{-1} h g = g_0 \in G_x$. Hence, $h = g g_0 g^{-1} \in g G_x g^{-1}$. This shows that $G_{gx} \subset g G_x g^{-1}$.

Conversely, suppose $g g_0 g^{-1} \in g G_x g^{-1}$, where $g_0 \in G_x$. Since $g_0 x = x$,

$$g g_0 g^{-1}(gx) = g g_0 x = gx.$$

This shows that $g g_0 g^{-1} \in G_{gx}$, so $g G_x g^{-1} \subset G_{gx}$. Therefore, $G_{gx} = g G_x g^{-1}$. □

Corollary. Let X be a G-set. If x and y are in the same G-orbit, then G_x and G_y are conjugate subgroups. In particular, $G_x \approx G_y$. □

The following result not only serves as a "counting theorem" in the finite case, but also says that up to equivalence, every G-set "looks like" a union of sets of cosets of G.

Theorem. Let X be a G-set, and let $x \in X$. There is a bijection $Gx \leftrightarrow G/G_x$. In particular, if G is finite, $|Gx| = |G/G_x| = (G : G_x)$: the order of the orbit equals the index of the isotropy group.

Proof. Define $\phi : Gx \to G/G_x$ by

$$\phi(gx) = gG_x.$$

I must check that ϕ is well-defined.

Suppose then that $g_1 x = g_2 x$. Then $g_2^{-1} g_1 x = x$, so $g_2^{-1} g_1 \in G_x$. Hence, $g_1 G_x = g_2 G_x$. Now

$$\phi(g_1 x) = g_1 G_x = g_2 G_x = \phi(g_2 x).$$

Therefore, ϕ is indeed well-defined.

Define $\psi : G/G_x \to Gx$ by

$$\psi(gG_x) = gx.$$

I must check that ψ is well-defined.

Suppose that $g_1 G_x = g_2 G_x$. Then $g_2^{-1} g_1 G_x = G_x$, so $g_2^{-1} g_1 \in G_x$. This means that $g_2^{-1} g_1 x = x$, or $g_1 x = g_2 x$. It follows that

$$\psi(g_1 G_x) = g_1 x = g_2 x = \psi(g_2 G_x).$$

Hence, ψ is well-defined.

Since ϕ and ψ are inverses, they are both bijections, and Gx and G/G_x are in 1-1 correspondence. □

Definition. Let X be a G-set, and let $S \subset G$. The **fixed point set** of X under S is

$$X^S = \{x \in X \mid gx = x \text{ for all } g \in S\}.$$

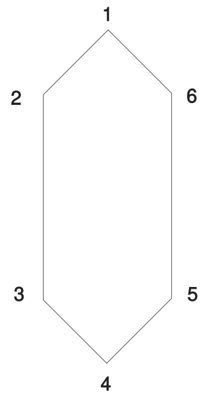
If $g \in G$, then X^g denotes the elements of X fixed by g: i.e. $X^g = \{x \in X \mid gx = x\}$.

Examples. 1. Consider the action of S_3 on the set $\{1,2,3\}$. Here is a picture of the isotropy groups and the fixed point sets:

	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
1	$\star$	$\cdot$	$\cdot$	$\star$	$\cdot$	$\cdot$
2	$\star$	$\cdot$	$\star$	$\cdot$	$\cdot$	$\cdot$
3	$\star$	$\star$	$\cdot$	$\cdot$	$\cdot$	$\cdot$

A $\star$ in a position means that the element of $\{1,2,3\}$ which labels the row is fixed by the element of S_3 which labels the column. $\square$

2. Consider the group of symmetries of the hexagon below:



Since the hexagon is not regular, the symmetry group has only 4 elements: the identity map (id), reflection across the x-axis (m_x), reflection across the y-axis (m_y), and rotation by π (r). The symmetry group acts on the set of vertices by permutations.

	id	m_x	m_y	r
1	$\star$	$\cdot$	$\star$	$\cdot$
2	$\star$	$\cdot$	$\cdot$	$\cdot$
3	$\star$	$\cdot$	$\cdot$	$\cdot$
4	$\star$	$\cdot$	$\star$	$\cdot$
5	$\star$	$\cdot$	$\cdot$	$\cdot$
6	$\star$	$\cdot$	$\cdot$	$\cdot$

This action is not transitive (unlike the action in the preceding example). The orbits are $\{1,4\}$ and $\{2,3,5,6\}$. $\square$

The following "counting theorem" relates the number of orbits under a group action to the size of the fixed point sets.

Theorem. (Burnside) Let X be a finite G-set, where G is a finite group. Then

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |X^g|.$$

Proof. Observe that $g \in G_x$ if and only if $x \in X^g$. It follows that

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|.$$

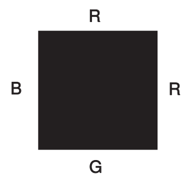
Now just compute:

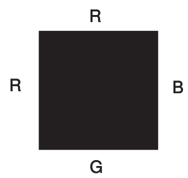
$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G_x|}{|G|} = \sum_{x \in X} \frac{1}{(G : G_x)} =$$

$$\sum_{x \in X} \frac{1}{|Gx|} = \sum_{K \in X/G} \sum_{x \in K} \frac{1}{|K|} = \sum_{K \in X/G} 1 = |X/G|. \square$$

Example. Each side of a square may be colored red, green, or blue. Colors may be repeated, and the square may be "turned over". How many distinct squares are there?

Note that since the square may be "turned over", the following colored squares are considered the same:





I'll temporarily nail the square to the wall so it can't move. There are then $3^4 = 81$ ways to paint the square. Two such paintings are "the same" if one can be carried into the other by a symmetry of the square — i.e., by an element of D_4.

Thus, X is the set of paintings of the fixed square. $G = D_4$ acts by symmetries. An equivalence class of paintings is simply an orbit under this action, and I want the number of orbits. According to Burnside, I simply count the number of fixed-square paintings (elements of X) fixed by each element of G.

element	id	r_1	r_2	r_3	m_x	m_y	m_+	m_-
fixed points	81	3	9	3	27	27	9	9

For example, m_x, reflection about the x-axis, fixes paintings where the top and bottom sides have the same color. Each side can be a different color, so there are $3 \cdot 3 \cdot 3 = 27$ paintings fixed by m_x.

The total number of fixed points is 168. Since $|D_4| = 8$, there are $168/8 = 21$ distinct paintings. $\square$

Conjugation action. The Class equation.

If X is a G-set, X is partitioned by the G-orbits. So if X is finite,

$$|X| = \sum_{x \in X/G} |Gx|.$$

("$x \in X/G$" means you should take one representative x from each orbit, and sum over *the set of representatives.* This is different from the notation "$K \in X/G$" which occurred in the proof of Burnside's Theorem; there I was actually summing over *the set of orbits.*)

x is a **fixed point** if $gx = x$ for all $g \in G$. In this case, x is an orbit all by itself. Recall that X^G denotes the set of fixed points of X. I can pull these one-point orbits out of the sum above to obtain

$$|X| = |X^G| + \sum_{x \in \Sigma} |Gx|.$$

In this case, Σ will denote the set of orbits which have more than one point. (I'll call them **nontrivial orbits** for short.) Thus, "$x \in \Sigma$" means that you should take one representative x from each nontrivial orbit.

Example. Here is a set X of 9 points arranged in a square:

$$\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{matrix}$$

Let the group D_4 of symmetries of the square act on X. There is one fixed point: 5. There are two nontrivial orbits: $\{1, 3, 7, 9\}$ and $\{2, 4, 6, 8\}$. The equation above says

$$9 = 1 + (4 + 4). \square$$

Lemma. If G is a group, G acts on itself by conjugation:

$$g \star x = gxg^{-1} \text{ for } g, x \in G.$$

Proof. $1 \star x = 1 \cdot x \cdot 1^{-1} = x$ for all $x \in G$. And if $a, b, c \in G$, then

$$(ab) \star x = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(b \star x)a^{-1} = a \star (b \star x).$$

Therefore, conjugation is an action. $\square$

Definition. The orbit of an element of G under the conjugation action is called a **conjugacy class**.

Remarks. I proved earlier that if x and y are two points in the same orbit, there is a $g \in G$ such that $g \star x = y$. It follows that any two elements in a conjugacy class are conjugate. $\square$

Example. Let $G = S_3$. The conjugacy classes are

$$\{\text{id}\}, \{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

(Note that if $x, y \in S_3$ and x and y are conjugate, then x and y are either both even or both odd.) $\square$

Lemma. Let G act on itself by conjugation, and let $x \in G$. Then $G_x = C(x)$, the centralizer of x.

Proof. Fix $x \in G$. When is $g \in G_x$? $g \in G_x$ means g fixes x, i.e. $gxg^{-1} = x$. This is equivalent to $gx = xg$, which in turn is what it means for x to be in $C(x)$. $\square$

Corollary. Let G act on itself by conjugation, and let $x \in G$. Then $|Gx| = (G : C(x))$.

Proof. The order of the orbit equals the index of the isotropy group, and I just showed the the isotropy group of x is $C(x)$. $\square$

Corollary. Let G act on itself by conjugation. Then $G^G = Z(G)$.

(The horrible notation G^G means the elements of G fixed under the conjugation action. I promise not to do it again.)

Proof. The orbit of a fixed point consists of the point itself, so $|Gx| = 1$. This is equivalent to $(G : C(x)) = 1$, or $G = C(x)$. This is the same as saying that everything commutes with x, i.e. $x \in Z(G)$. $\square$

I'll apply these results to the equation

$$|X| = |X^G| + \sum_{x \in \Sigma} |Gx|.$$

In this case, the G-set is $X = G$. The set of fixed points is the center: $X^G = Z(G)$. The nontrivial orbits Σ consist of conjugacy classes with more than one element. The order of such a conjugacy class is $(G : C(x))$, where $C(x)$ is the centralizer of x. (I must take one such x for each nontrivial orbit.) Therefore,

$$|G| = |Z(G)| + \sum_{x \in \Sigma} (G : C(x)).$$

This is called the **class equation**.

Example. Let $G = S_3$. The center of S_3 is $Z(S_3) = \{\text{id}\}$, and the nontrivial conjugacy classes are

$$\{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

Take one element from each nontrivial class: say $(1\ 2)$ and $(1\ 2\ 3)$. Their centralizers are

$$C\left((1\ 2)\right) = \{\text{id}, (1\ 2)\} \text{ and } C\left((1\ 2\ 3)\right) = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}.$$

Thus,

$$|Z(S_3)| + \left(S_3 : C\left((1\ 2)\right)\right) + \left(S_3 : C\left((1\ 2\ 3)\right)\right) = 1 + 3 + 2 = 6 = |S_3|. \square$$

Example. Consider the group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ of quaternions. Here are the conjugacy classes:

$$\text{central elements:} \quad \{1\}, \{-1\}$$

$$\text{nontrivial conjugacy classes:} \quad \{i, -i\}, \quad \{j, -j\}, \quad \{k, -k\}$$

I found these by direct computation. For example, the conjugates of i are:

$$\begin{array}{ll} 1 \cdot i \cdot (-1) = -i & (-1) \cdot i \cdot 1 = -i \\ i \cdot i \cdot (-i) = -i & (-i) \cdot i \cdot i = -i \\ j \cdot i \cdot (-j) = -i & (-j) \cdot i \cdot j = -i \\ k \cdot i \cdot (-k) = -i & (-k) \cdot i \cdot k = -i \end{array}$$

Hence, $\{i, -i\}$ is a complete conjugacy class.

In the class equation, the sum is taken over a set of representatives Σ for the nontrivial conjugacy classes. In this example, for instance, I could take $\Sigma = \{i, j, k\}$ or $\Sigma = \{-i, -j, k\}$ or … — i.e. any three elements, one from each of the (nontrivial) classes $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$.

Finally, note that $|Z(Q)| = 2$, and the nontrivial classes have 2, 2, and 2 elements, respectively. The class equation says (correctly) that

$$2 + (2 + 2 + 2) = 8. \square$$

Before I prove the next result, I'll review some things that are apparent from the derivation of the class equation. I had G acting on itself by conjugation. Then an orbit Gx (which does *not* mean "G times x" in this case!) is the conjugacy class of x — i.e. the set of elements conjugate to x. Assuming that G is finite, the order of the orbit equals the index of of the isotropy group, so $|Gx| = (G : C(x))$, where $C(x)$ is the centralizer of x — the set of elements which commute with x.

In the $\sum_{x\in\Sigma}(G : C(x))$ term, I'm summing over conjugacy classes *with more than one element.* This implies two things:

1. $(G : C(x)) > 1$, because $(G : C(x))$ equals the number of elements in the conjugacy class.
2. $|C(x)| < |G|$, since $|G| = (G : C(x))|C(x)|$, and $(G : C(x)) > 1$.

Definition. Let p be prime. G is a p-group if for all $g \in G$, $g \neq 1$, the order of g is p^n for some $n > 0$. (n may be different for different elements.)

Finite p-groups are an important class of finite groups. Their structure is described in some detail by **Sylow theory**. Sylow theory is also an important tool in determining the structure of arbitrary finite groups. For example, it provides tools that helps answer questions like: How many different groups of order 20 are there?

As applications of the class equation, I'll look at two results that are "preliminaries" to Sylow theory.

The first result says that if p is prime and $p \mid |G|$, then G has an element of order p. Note that if n is not prime, $n \mid |G|$ does not imply the existence of an element of order n. Trivial counterexample: $|\mathbb{Z}_3 \times \mathbb{Z}_3| = 9$, which is divisible by 9, but $\mathbb{Z}_3 \times \mathbb{Z}_3$ has no elements of order 9.

Lemma. Let G be a finite abelian group, and let p be a prime number which divides $|G|$. Then G has an element of order p.

Proof. Induct on $|G|$. Observe that $\mathbb{Z}_2$ has an element of order 2 and $\mathbb{Z}_3$ has an element of order 3 (and those are the only groups of order 2 and 3, respectively). This gets the induction started.

Now suppose $n > 3$, and assume the result is true for abelian groups of order less than n. Let $|G| = n$, $p \mid n$. I want to show that G has an element of order p.

Let $x \in G$, where $x \neq 0$. If x has order pk for some k, then kx has order p. Therefore, assume that the order of x is not divisible by p.

Now $\langle x\rangle \neq G$, else x has order n, and n is divisible by p by assumption. Now

$$p \mid |G| = (G : \langle x\rangle)|\langle x\rangle|.$$

Since $p \not| \, |\langle x\rangle|$,

$$p \mid (G : \langle x\rangle) = \left|\frac{G}{\langle x\rangle}\right|.$$

Now $|G/\langle x\rangle| < |G|$ since $|\langle x\rangle| > 1$, so $G/\langle x\rangle$ is an abelian group of order less than $|G|$ whose order is divisible by p. By the induction hypothesis, $G/\langle x\rangle$ contains an element $y + \langle x\rangle$ of order p, where $y \in G$.

Suppose y has order m. Then

$$my = 0, \quad my + \langle x\rangle = \langle x\rangle, \quad m(y + \langle x\rangle) = \langle x\rangle = 0 \in \frac{G}{\langle x\rangle}.$$

Since m kills $y + \langle x\rangle$, it follows that m is divisible by the order p. Suppose $m = kp$. Then ky has order p.

This shows that G has an element of order p and completes the induction. $\square$

Theorem. (Cauchy) Let G be a finite group, and let p be a prime number which divides $|G|$. Then G has an element of order p.

Proof. Induct on $|G|$. Observe that $\mathbb{Z}_2$ has an element of order 2 and $\mathbb{Z}_3$ has an element of order 3 (and those are the only groups of order 2 and 3, respectively). This gets the induction started.

Now suppose $n > 3$, and assume the result is true for groups of order less than n. Let $|G| = n$, $p \mid n$. I want to show that G has an element of order p.

Consider $x \in \Sigma$, so the conjugacy class of x contains more than one element. By the remarks preceding the lemma, $|C(x)| < |G|$. By induction, if $p \mid |C(x)|$, then $C(x)$ has an element of order p. Since $C(x) < G$, I'll then have an element of order p in G.

Therefore, assume that $p \not| \, |C(x)|$, for all $x \in \Sigma$. Now

$$p \mid |G| = (G : C(x))|C(x)|.$$

Hence, $p \mid (G : C(x))$ for all $x \in \Sigma$. Look at the class equation

$$|G| = |Z(G)| + \sum_{x \in \Sigma} (G : C(x)).$$

p divides each term in the summation, and p divides $|G|$ by assumption. Therefore, $p \mid |Z(G)|$. However, $Z(G)$ is an abelian group, so the Lemma shows that it has an element of order p. Since $Z(G) < G$, G has an element of order p as well. □

Corollary. Let p be prime. The order of a finite p-group is p^n for some $n > 0$.

Proof. If G is a finite p-group, every element has order equal to a power of p. If $|G| \neq p^n$ for some n, then $q \mid |G|$, where q is a prime number and $q \neq p$. By Cauchy's theorem, G has an element of order q $\times$. Therefore, $|G| = p^n$ for some n. □

Proposition. Let p be prime. The center of a nontrivial finite p-group is nontrivial.

Proof. Examine the class equation

$$|G| = |Z(G)| + \sum_{x \in \Sigma} (G : C(x)).$$

Since $|G| = p^n$ for some $n > 0$, $p \mid |G|$. If $x \in \Sigma$, the remarks preceding the lemma above show that $(G : C(x)) > 1$. Since $p^n = |G| = (G : C(x))|C(x)|$, it follows that $p \mid (G : C(x))$. Now p divides $|G|$ and every term in the summation, so p divides $|Z(G)|$. Therefore, $|Z(G)| \neq 1$. □

