4. p-groups and the class formula

The class formula is used to prove that p-groups are nilpotent. The class formula in turn comes from the orbit-stabilizer formula.

4.1. **orbit-stabilizer formula.**

This follows from the following theorem.

Theorem 4.1. *Suppose that G acts on a set X and $x \in X$. Then there is a bijection between the orbit $\pi_G(x)$ of x and the set of left cosets of the stabilizer G_x of x. The bijection*

$$\phi : G/G_x \xrightarrow{\approx} \pi_G(x)$$

is given by $\phi(gG_x) = gx$.

When X is finite, we get a numerical formula.

Corollary 4.2 (orbit-stabilizer formula)**.** *If X is a G-set and $x \in X$, the size of the orbit of x is equal to the index of the stabilizer of x.*

Recall that X is a disjoint union of orbits:

$$X = \coprod_{x_i \ rep} \pi_G(x_i)$$

where $x_i \in X$ are representatives of the orbits (i.e., one element from each orbit).

Corollary 4.3 (orbit-sum formula)**.** *The number of elements in a finite G-set X is given by*

$$|X| = \sum_{x_i \ rep} |\pi_G(x_i)| = \sum_{x_i \ rep} |G : G_{x_i}|.$$

4.2. **actions of p-groups.**

One example of the orbit-sum formula is given by the action of p-groups on finite sets. If P is a p-group, with $|P| = p^k$ then every subgroup has order a power of p. If P acts on a finite set X then the size of each orbit is also a power of p:

$$|\pi_P(x)| = |P : P_x| = \frac{|P|}{|P_x|} = \frac{p^k}{p^j} = p^{k-j}.$$

Notice that this is divisible by p except when it is equal to 1. The size of X is given by the orbit-sum formula:

$$|X| = \sum_{x_i} |P : P_{x_i}| = \sum_{x_i} p^{k-j_i}.$$

Now we want to separate the summands which are equal to 1 and those which are greater than 1. If $|P : P_x| = 1$ then $P_x = P$ and x is a *fixed* *point* of the action. This means $g \cdot x = x$ for all $g \in P$. The other orbits have more than one element and therefore the size of these orbits is divisible by p. This gives the following theorem which we need later.

Theorem 4.4. *Suppose that P is a p-group acting on a finite set X. Then the number of elements in X is congruent modulo p to the number of fixed points of the action.*

The key use of this formula is the following.

Corollary 4.5. *Every nontrivial finite p-group has a nontrivial center.*

Proof. Suppose that P is a p-group with $p^k > 1$ elements. Then P acts on P by conjugation. The theorem says that the number of fixed points of this action is congruent to $|P| = p^k$ module p. In other words, p divides the number of fixed points. But $g \in P$ is a fixed point of the conjugation action if and only if $g \in Z(P)$. Therefore, p divides $|Z(P)|$ which implies that $Z(P)$ has at least p elements. □

4.3. **class formula.** This is another example of the orbit-sum formula. Take a finite group G acting on the set G by conjugation. Then the orbit of $x_i \in G$ is the conjugacy class of x_i and the stabilizer is the centralizer $C_G(x_i)$ of x_i. This gives the following formula.

$$|G| = \sum_{x_i} |\gamma_G(x_i)| = \sum_{x_i} |G : C_G(x_i)|$$

This is not the class formula. We need to separate the summands which are equal to 1. By the orbit-stabilizer formula,

$$|\gamma_G(x)| = |G : G_x| = |G : C_G(x)| = 1$$

This means $C_G(x) = G$. In other words, x is central, or $x \in Z(G)$. You can also just look at the definition:

$$\gamma_G(x) = \{gxg^{-1} \mid g \in G\}.$$

This is $\{x\}$ if and only if $gxg^{-1} = x$, i.e., $x \in Z(G)$.

Every central element contributes 1 to the sum and every noncentral element contributes a number $|G : C_G(x)| \neq 1$. This gives the following.

Theorem 4.6 (class formula)**.** *The number of elements in any finite group G is given by*

$$|G| = |Z(G)| + \sum_{x_i} |\gamma_G(x_i)| = |Z(G)| + \sum_{x_i} |G : C_G(x_i)|$$

where the x_i are representatives of the conjugacy classes in G which contain more than one element.

This formula is used to prove Corollary 4.5 but we already did that.

5. Nilpotent groups

There are two definitions of nilpotent groups. I don't remember whether I proved that they are equivalent but we can do that here.

Definition 5.1. *A group G is* nilpotent *if there is a normal tower*

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$$

with the following properties for all i.

(1) $G_i \trianglelefteq G$ *and*
(2) $G_{i-1}/G_i \leq Z(G/G_i)$.

A normal tower satisfying these conditions will be called a central series.

The smallest possible value of n is called the *nilpotency class* of G. Thus G has nilpotency class 1 if and only if it is abelian (and nontrivial).

The other definition that I gave used iterated centers $Z^{(i)}(G)$ defined recursively as follows.

(1) $Z^{(1)}(G) := Z(G)$.
(2) $Z^{(n+1)}(G)$ is the unique normal subgroup of G which contains $Z^{(n)}(G)$ and so that

$$\frac{Z^{(k+1)}(G)}{Z^{(k)}} = Z\left(\frac{G}{Z^{(k)}(G)}\right)$$

Notice that this recursive definition implies that

$$\frac{Z^{(n)}(G)}{Z(G)} = Z^{(n-1)}\left(\frac{G}{Z(G)}\right). \tag{5.1}$$

Proposition 5.2. *A group G is nilpotent if and only if $G = Z^{(n)}(G)$ for some n. Furthermore, the smallest such n is equal to the nilpotency class of G.*

Proof. If $G = Z^{(n)}(G)$ then the tower

$$G = Z^{(n)}(G) \geq Z^{(n-1)}(G) \geq \cdots \geq Z(G) \geq \{e\}$$

is a central series. Therefore, G is nilpotent of class $c \leq n$.

Conversely, suppose that G is nilpotent of class c. Then we have a central series:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{c-1} \trianglerighteq G_c = \{e\}$$

Claim: $G_{c-k} \leq Z^{(k)}(G)$ for all k.

If this is true then, putting $k = c$, we get the that $G = Z^{(c)}(G)$, which means that $c \geq n$ where n is the smallest number satisfying

$G = Z^{(n)}(G)$. Since $c \geq n$ and $c \leq n$ we conclude that $c = n$. So, it suffices to prove the claim.

The claim holds for $k = 1$ by the assumption that G_i form a central series. Suppose by induction on k that $G_{c-k} \leq Z^{(k)}(G)$ and we have the quotient map:

$$\phi : G/G_{c-k} \twoheadrightarrow G/Z^{(k)}(G).$$

Any epimorphism has the property that it sends central elements into central elements. Therefore,

$$\phi\left(\frac{G_{c-k-1}}{G_{c-k}}\right) \leq \phi\left(Z\left(\frac{G}{G_{c-k}}\right)\right) \leq Z\left(\frac{G}{Z^{(k)}(G)}\right) = \frac{Z^{(k+1)}(G)}{Z^{(k)}}.$$

Since ϕ is the quotient map this implies that $G_{c-k-1} \leq Z^{(k+1)}(G)$. Therefore, the claim and thus the proposition holds. □

Corollary 5.3. *A nontrivial group G is nilpotent of class c if and only if $G/Z(G)$ is nilpotent of class $c-1$.*

Proof. This follows from the proposition and Equation (5.1). G is nilpotent of class $\leq c$ if and only if $Z^{(c)}(G) = G$. By (5.1) this is equivalent to saying that $Z^{(c-1)}(G/Z(G)) = G/Z(G)$. By the proposition the last statement is equivalent to saying that $G/Z(G)$ is nilpotent of class $\leq c-1$. Putting these together we get the corollary. □

Corollary 5.4. *Finite p-groups are nilpotent.*

Proof. If P is a p-group then $|P| = p^k$ for some k. If $k = 1$ then P is cyclic and therefore abelian making it nilpotent of class 1. If $k > 1$ then P has a nontrivial center $Z(P)$ and $P/Z(P)$ is nilpotent by induction. By the previous corollary this implies that P is nilpotent. □