The Class Equation

Let G be a group. The set of all elements x that have the property that $x\bigstar a = a\bigstar x$ for every a in G is called the center of G. We will use the symbol Z for the center of a group. While there is some chance that you might confuse this symbol with the symbol for a modular group Z_n, the only other widely used symbol for the center of a group is C which we will put to a different use. $\therefore Z = \{x | x \in G \text{ and } x\bigstar a = a\bigstar x \text{ for every } a \in G\}$. In other words, the center of a group is the set of elements that commute with all other elements. Please note that in any group, $e \in Z$. Thus, the center of a group is never the empty set.

Example 1: The center of any abelian group is the entire group.

Example 2: If $G = D_4$ then $Z = \{e, b^2\}$. This can be confirmed by a quick inspection of the b^2 row and column of your group table for D_4.

Example 3: If $G = Q_8$ then $Z = \{1, \text{-}1\}$.

Theorem: Let G be a group. Let Z be its center. Z is a normal subgroup of G.

Proof:

Closure

Let z_1 and z_2 be elements of Z. We must prove that $z_1 \cdot z_2 \in Z$. Let $a \in G$. Consider:

$$\begin{aligned}
(z_1 \cdot z_2) \cdot a &= z_1 \cdot (z_2 \cdot a) \\
&= z_1 \cdot (a \cdot z_2) \text{ since } z_2 \in Z \\
&= (z_1 \cdot a) \cdot z_2 \\
&= (a \cdot z_1) \cdot z_2 \text{ since } z_1 \in Z \\
&= a \cdot (z_1 z_2)
\end{aligned}$$

$$\therefore (z_1 \cdot z_2) \cdot a = a \cdot (z_1 \cdot z_2)$$

$$\therefore z_1 \cdot z_2 \in Z$$

Inverse Closure

Let $z \in Z$. We must prove $z^{-1} \in Z$. For any a in G, we know:

$$az = za$$

$$\therefore z^{-1}az = a$$

$$\therefore z^{-1}a = az^{-1}$$

$$\therefore z^{-1} \in Z$$

NTC

Let $a \in G$, let $z \in Z$. Consider:

$$\begin{aligned} aza^{-1} &= zaa^{-1} \\ &= ze \\ &= z \in Z \\ \therefore aza^{-1} &\in Z \\ \therefore Z &\lhd G \end{aligned}$$

QED

Definition: Let G be a group. Let $a \in G$. The centralizer of a (denoted $C(a)$) is defined to be the set of all elements x in G such that $x \cdot a = a \cdot x$.

Note that for any group G and any element a in it, $Z \subseteq C(a)$. Note also that $C(a)$, for $a \neq e$, always contains at least two elements. $e \in C(a)$ since $e \cdot a = a \cdot e$ always. Also $a \in C(a)$ since $a \cdot a = a \cdot a$. If $a^{-1} \neq a$, then a^{-1} is a third element of $C(a)$ since $a \cdot a^{-1} = a^{-1} \cdot a$ always. For any group, if $x \in Z$ then $C(x) = G$. Finally, if G is an abelian group then $C(a) = G$ for any a.

Example 1: In Q_8, $C(i) = \{1.-1, i, -i\}$.

Example 2: In D_4, $C(b) = \{e, b, b^2, b^3\}$.

Example 3: In Z_6, $C(2) = Z_6$.

Theorem: Let G be a group. Let $a \in G$. $C(a)$ is a subgroup of G.

Proof: Let x_1 and x_2 be elements of $C(a)$. Consider :

$$\begin{aligned} &(x_1x_2)a = x_1(x_2a) = x_1(ax_2) \\ &= (x_1a)x_2 = (ax_1)x_2 = a(x_1x_2) \\ &\therefore (x_1x_2)a = a(x_1x_2) \\ &\therefore x_1x_2 \in C(a) \end{aligned}$$

Inverse Closure

Let $x \in$ C(a)
By definition $ax = xa$

$$\begin{aligned} &\Rightarrow a = xax^{-1} \\ &\Rightarrow x^{-1}a = ax^{-1} \\ &\therefore x^{-1} \in C(a) \end{aligned}$$

QED

For a given group G and element a, $C(a)$ may not be normal. If G is finite, $o(C(a))$ has to be a divisor of $o(G)$ as is the case for any subgroup. The right cosets generated by $C(a)$ partition the group into disjoint subsets and the right cosets all have the same order. The same can be said for the left coset. For an example of a centralizer that is not normal, consider a in D_3. $C(a) = \{e, a\}$ which we know by previous calculations is not normal in D_3.

Definition: Let G be a group. Let $a \in G$. An element b in G is said to be conjugate to a if and only if there exists an element x in G such that $b = xax^{-1}$.

If G is an abelian group, the only element conjugate to a is a itself since $xax^{-1} = xx^{-1}a = a$ for any a. Further, if a is in the center of a non-abelian group, then once again the only conjugate of a is a itself for the same reason. To discover the set of all conjugates of a given element a by brute force one needs to compute xax^{-1} for every x in G.

Theorem: Let G be a group. Define a relation R on G by: aRb iff a is conjugate to b, i.e. iff there exists x in G such that $a = xbx^{-1}$. R is an equivalence relation.

Reflexive Property

Since $eae^{-1} = eae = a$ for any a, a is a conjugate to itself. $\therefore aRa$ for any a in G.

Symmetric Property

Suppose aRb. There exists x such that $a = xbx^{-1}$.

$\Rightarrow x^{-1}a = bx^{-1}$

$\Rightarrow x^{-1}ax = b$

Let $y = x^{-1}$. We know that $y^{-1} = (x^{-1})^{-1} = x$

$\therefore yay^{-1} = b$

$\therefore b$ is conjugate to a

$\therefore bRa$

Transitive Property

Suppose aRb and bRc.

There exists x_1 such that $a = x_1bx_1^{-1}$. There exists x_2 such that $b = x_2cx_2^{-1}$.

Consider:

$a = x_1bx_1^{-1}$

$a = x_1x_2cx_2^{-1}x_1^{-1}$

$a = (x_1x_2)c(x_1x_2)^{-1}$

Let $x_1x_2 = x_3$

Then: $a = x_3cx_3^{-1}$

$\therefore aRc$

QED

As we know, all equivalence relations induce equivalence classes on the set upon which they are defined. By an early theorem in this text, two equivalence classes are either equal or disjoint. We can see that any collection of distinct equivalence classes that have the property that every element in the set is in exactly one equivalence class acts as a partition of the original set. We have seen this before when we partitioned a group into cosets induced by a particular subgroup. However, partitioning a group by cosets is far different from partitioning a group by conjugacy. If the group is finite,the order of any one coset is the same as any other coset. However, as we are about to see, partitioning a finite group using conjugate classes creates disjoint or equal subsets that do not have the same order. In other words, if a and b are elements of a finite group G, then the order of the conjugate class generated by a may well be different that the order of the conjugate class generated by b.

First a definition. The conjugate class of an element a in a set G (denoted $cl(a)$ is defined to be the set of all elements conjugate to a. In other words:
Definition: $cl(a) = \{b | b = xax^{-1} \text{ for some } x \in G\}$

Example 1: Let $G = D_3 = \{e, a, b, b^2ab, ab^2\}$.

$$cl(e) = \{e\} \text{ since } xex^{-1} = e \text{ for all } x$$

$$\begin{aligned} cl(a) &= \left\{eae^{-1}, aaa^{-1}, bab^{-1}, (b^2)a(b^2)^{-1}, (ab)a(ab)^{-1}, (ab^2)a(ab^2)^{-1}\right\} \\ &= \{a, ab, ab^2\} \end{aligned}$$

$$\begin{aligned} cl(b) &= \left\{ebe^{-1}, aba^{-1}, bbb^{-1}, b^2b(b^2)^{-1}, (ab)b(ab)^{-1}, (ab^2)b(ab^2)^{-1}\right\} \\ &= \{b, b^2\} \end{aligned}$$

$$cl(b^2) = \{b, b^2\}$$

$$cl\{ab\} = \{a, ab, ab^2\}$$

$$cl\{ab^2\} = \{a, ab, ab^2\}$$

You should verify each of these results! D_4 is the union of distinct classes and $o(D_4)$ is the sum of the orders of the distinct classes.

We could say:

$$o(D_4) = o(cl(e)) + o(cl(a)) + o(cl(b))$$

or

$$o(D_4) = o(cl(e)) + o(cl(ab^2)) + o(cl(b^2))$$

We could not say:

$$o(D_4) = o(cl(e)) + o(cl(a)) + o(cl(b)) + o(cl(b^2)) + o(cl(ab)) + o(cl(ab^2))$$

The two equations above for $o(D_4)$ will soon be examples of a principle called the "class equation".

Example 2: Let $G = Q_8 = \{1, \text{-}1, i, \text{-}i, j, \text{-}j, k, \text{-}k\}$

$$cl(1) = \{1\}$$
$$cl(\text{-}1) = \{\text{-}1\}$$
$$cl(i) = \{i, \text{-}i\}$$
$$cl(\text{-}i) = \{i, \text{-}i\}$$
$$cl(j) = \{j, \text{-}j\}$$
$$cl(\text{-}j) = \{j, \text{-}j\}$$
$$cl(k) = \{k, \text{-}k\}$$
$$cl(\text{-}k) = \{k, \text{-}k\}$$

Therefore, $\text{o}(Q_8) = \text{o}(cl(1)) + \text{o}(cl(\text{-}1)) + \text{o}(cl(\text{-}i)) + \text{o}(cl(\text{-}j)) + \text{o}(cl(k))$ or any of a number of other representations as the sum of orders of disjoint conjugacy classes.

The preliminary "class equation" we have derived by knowing that conjugacy is an equivalence relation is:

Class Equation Part I: If G is a finite group then $\text{o}(G) = \sum_{a \in G} \text{o}(cl(a))$ where the sum includes each equivalence class once and only once. In other words, if a is conjugate to b and $\text{o}(cl(a))$ is one of the addends in the sum then $\text{o}(cl(b))$ is not one of the addends.

Theorem: Let G be a group. Let $p \in G$. $cl(p) = \{p\}$ if and only if p is an element of Z, the center of G.

Proof: If $p \in Z$ then $xpx^{-1} = pxx^{-1} = p$ for all x.

$\therefore cl(p) = \{p\}$

Conversely, suppose $cl(p) = \{p\}$.

Then, $xpx^{-1} = p$ for all $x \in G$.

$\therefore xp = px$ for all $x \in G$

$\therefore p \in Z$

QED

We now know that any time the conjugacy class of an element is a singleton then that element is a center element. The union of the singleton subsets must yield the entire center of the group. Therefore, $\text{o}(Z) = \sum \text{o}(cl(c))$ where the sum is computed for each center element c. Note that for each such c, $\text{o}(cl(c)) = 1$.

Class Equation Part II: If G is a finite group, $\text{o}(G) = \text{o}(Z) + \sum \text{o}(cl(a))$ where Z is the center of G and the sum on the right assumes each conjugate class is represented once and only once and each a in that sum is not an element of Z. For Q_8, we obtain:

$$\text{o}(G) = \text{o}(Z) + \text{o}(cl(i)) + \text{o}(cl(j)) + \text{o}(cl(k)) \text{ where } Z = \{i, \text{-}i\}.$$

We will now establish a relationship between the centralizer of an element and the conjugate class of that element for finite groups. We proved that $C(a)$ is a subgroup. All subgroups generate left cosets which are disjoint or equal and whose orders in a finite group are identical. The number of left cosets generated by $C(a)$ is given by $\frac{o(G)}{o(C(a))}$.

Suppose $xC(a) = yC(a)$
$\Rightarrow x \in yC(a)$
$\Rightarrow x = yr$ for some $r \in C(a)$
$\therefore xax^{-1} = (yr)a(yr)^{-1} = yrar^{-1}y^{-1}$
$= yarr^{-1}y^{-1}$ [since $r \in C(a)$]
$= yay^{-1}$
$\therefore x$ and y generate the same conjugate of a.

Conversely, suppose x and y generate the same conjugate of a. Then:
$xax^{-1} = yay^{-1}$
$\Rightarrow y^{-1}xa = ay^{-1}x$
$\Rightarrow y^{-1}x \in C(a)$
$\Rightarrow x \in yC(a)$
$\Rightarrow xC(a) = yC(a)$

We have proven that the number of conjugates of a equals the number of left cosets generated by $C(a)$.

$$\therefore o(cl(a)) = \frac{o(G)}{o(C(a))}$$

Class Equation Part III: For any finite group G,

$$o(G) = o(Z) + \sum \frac{o(G)}{o(cl(a))}$$

where Z is the center of G and each conjugate class is represented once and only once in the summation.