Lecture 11: The conjugates of an element

Let x be a (fixed) element of a group G, and let g be any element. We know that g commutes with x, or centralizes x, or belongs to the centralizer of x, if and only if

$$xg = gx \text{ in } G.$$

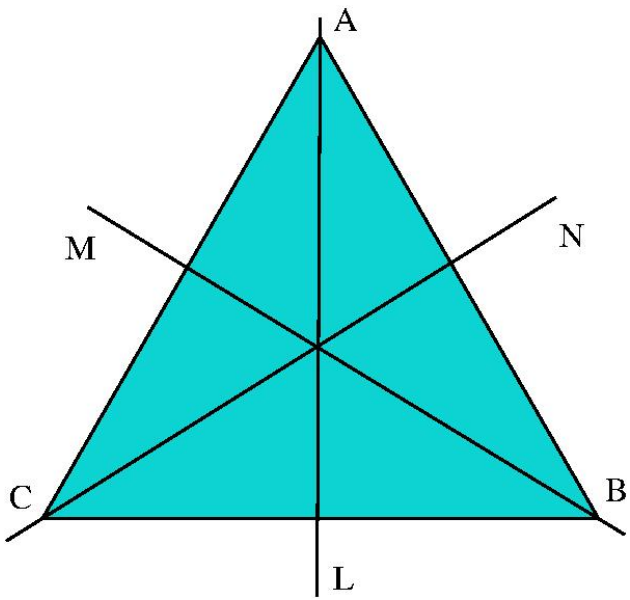
The equation $xg = gx$ can be rearranged (after composing on the right with g^{-1} on both sides) to

$$x = gxg^{-1}.$$

As g moves through the elements of G, the element gxg^{-1} is equal to x only when $g \in C_G(x)$. All of the elements that occur as gxg^{-1}, as g varies, are called the conjugates of x in G.

Context and Examples

1. Let A be a matrix in $\mathrm{GL}(3,\mathbb{R})$. The conjugates of A in $\mathrm{GL}(3,\mathbb{R})$ are all matrices of the form PAP^{-1}, where P is an invertible matrix. These are exactly the matrices that represent the same linear transformation as A, with respect to different choices of basis.
2. Let G be the group D_6 of symmetries of the equilateral triangle.



- Conjugates of id: just id itself.
- Conjugates of R_{120}: R_{120} and R_{240}.
  If T is a reflection, then
  $T \circ R_{120} \circ T^{-1} = R_{240}$.
- Conjugates of T_L: T_L, T_M and T_N.
  $R_{120} \circ T_L \circ R_{120}^{-1} = T_N$.
  $R_{240} \circ T_L \circ R_{240}^{-1} = T_M$.

Conjugacy is an equivalence relation

In a group G, write $x \sim y$ to mean that y is a conjugate of x, i.e. that $y = gxg^{-1}$ for some $g \in G$.

- $\sim$ is reflexive: $x \sim x$ for all $x \in G$, since $x = xxx^{-1}$.
- $\sim$ is symmetric
  Suppose $x \sim y$ and write $y = gxg^{-1}$, where $g \in G$.
  Then $x = g^{-1}yg = g^{-1}y(g^{-1})^{-1}$, so $y \sim x$ and $\sim$ is symmetric.
- $\sim$ is transitive.
  Suppose $x \sim y$ and $y \sim z$. Then we can write $y = gxg^{-1}$ and $z = hyh^{-1}$, where $g, h \in G$. We want to show $x \sim z$. Note

$$z = hyh^{-1} = h(gxg^{-1})h^{-1} = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}.$$

  So $x \sim z$ and $\sim$ is transitive.

Conjugacy Classes

Recall that elements x and y in a group G are conjugate to each other if

$$y = gxg^{-1} \text{ for some } g \in G.$$

The set of elements of G that are conjugate to x in G is called the conjugacy class of x, which we denote here by $\mathrm{Cl}(x)$. Because conjugacy is an equivalence relation on G, conjugacy classes of different elements are either equal or disjoint:

- $\mathrm{Cl}(x) = \mathrm{Cl}(y)$ if x and y are conjugates of each other.
- $\mathrm{Cl}(x) \cap \mathrm{Cl}(y) = \emptyset$ if x and y are not conjugates of each other.

Note For $x \in G$, $\mathrm{Cl}(x) = \{x\}$ if and only if $x \in Z(G)$.
An element of the centre of G has only one conjugate in G, namely itself.

How many conjugates does x have? (Theorem 2.2.9)

Let $x \in G$. Then every element of the form gxg^{-1}, where $g \in G$, is a conjugate of x in G, but they need not be distinct.

When is $g_1 x g_1^{-1} = g_2 x g_2^{-1}$?

$$\begin{aligned} g_1 x g_1^{-1} &= g_2 x g_2^{-1} \\ \iff g_1 x &= g_2 x g_2^{-1} g_1 \\ \iff g_2^{-1} g_1 x &= x g_2^{-1} g_1 \\ \iff (g_2^{-1} g_1) x &= x (g_2^{-1} g_1) \end{aligned}$$

So the conjugates $g_1 x g_1^{-1}$ and $g_2 x g_2^{-1}$ are the same element if and only if $g_2^{-1} g_1 \in C_G(x)$. This occurs if and only if g_1 and g_2 belong to the same left coset of $C_G(x)$ in G.

Conclusion The number of distinct conjugates of x in G is $[G : C_G(x)]$, the index in G of the centralizer of x. Note that this means the number of elements in any conjugacy class is a divisor of $|G|$.

The Class Equation

Let G be a finite group. Then the number of elements of G is the sum of the numbers of elements of all of the conjugacy classes in G, all of which are divisors of $|G|$. This can be written as

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

where there is one x_i from each class with more than one element.

Consequence If the order of G is a prime power (like 3^7 or 5^3), the center of G cannot be trivial.
Suppose $|G| = p^k$ for some prime p. Then

$$p^k = |Z(G)| + \sum_i [G : C_G(x_i)].$$

We know that $|Z(G)| \geq 1$, we want to show $|Z(G)| \neq 1$. Every other term in the above equation is a multiple of p, so $Z(G)$ must be a multiple of p too, and $Z(G)$ is not the trivial subgroup of G.