2.2 The centre, centralizers and conjugacy

Definition 2.2.1. *Let* G *be a group with operation* $\star$*. The* centre *of* G*, denoted by* $Z(G)$ *is the subset of* G *consisting of all those elements that commute with* every *element of* G*, i.e.*

$$Z(G) = \{x \in G : x \star g = g \star x \text{ for all } g \in G\}.$$

Note that the centre of G is equal to G if and only if G is abelian.

Example 2.2.2. *What is the centre of* $GL(n, \mathbb{Q})$*, the group of* $n \times n$ *invertible matrices with rational entries (under matrix multiplication)?*

Solution (Summary): Suppose that A belongs to the centre of $GL(n, \mathbb{Q})$ (so A is a $n \times n$ invertible matrix). For i, j in the range $1, \dots, n$ with $i \neq j$, let E_{ij} denote the matrix that has 1 in the (i, j) position and zeros in all other positions. Then $I_n + E_{ij} \in GL(n, \mathbb{Q})$ and

$$A(I_n + E_{ij}) = (I_n + E_{ij})A \implies A + AE_{ij} = A + E_{ij}A \implies AE_{ij} = E_{ij}A.$$

Now AE_{ij} has Column i of A as its jth column and is otherwise full of zeros, while $E_{ij}A$ has Row j of A as its ith row and is otherwise full of zeros. In order for these two matrices to be equal for all i and j, it must be that the off-diagonal entries of A are all zero and that the entries on the main diagonal are all equal to each other. Thus $A = aI_n$, for some $a \in \mathbb{Q}$, $a \neq 0$. On the other hand it is easily checked that any matrix of the form aI_n where $a \in \mathbb{Q}$ *does* commute with all other matrices. Hence the centre of $GL(n, \mathbb{Q})$ consists precisely of those matrices aI_n where $a \in \mathbb{Q}$, $a \neq 0$.

Note: Matrices of this form are called *scalar* matrices, they are scalar multiples of the identity matrix.

Exercise: Write out an expanded version of the above proof yourself, making sure that you follow all the details. Proofs like this that involve matrix indices and the mechanism of matrix multiplication tend to be fairly concise to write down but also fairly intricate for the reader to unravel.

A key fact about the centre of a group is that it is not merely a subset but a *subgroup*. This is our first example of a subgroup that is defined by the behaviour of its elements under the group operation.

Theorem 2.2.3. *Let* G *be a group. Then* $Z(G)$ *is a subgroup of* G*.*

Proof. We have the usual three things to show, and we must use the definition of the centre to show them.

- $Z(G)$ is closed under the operation of G.
  Suppose $a, b \in Z(G)$. We must show that $ab \in Z(G)$. That means showing that for any element x of G, x commutes with ab. Now

  $$\begin{aligned} abx &= axb \ (bx = xb \text{ since } b \in Z(G)) \\ &= xab \ (ax = xa \text{ since } a \in Z(G)). \end{aligned}$$

  So $abx = xab$ for all $x \in G$, and $ab \in Z(G)$.

- $\mathrm{id}_G \in Z(G)$
  By definition $\mathrm{id}_G x = x\mathrm{id}_G = x$ for all $x \in G$, so id_G commutes with every element of G and belongs to the centre of G.

- Suppose $a \in Z(G)$. We need to show that $a^{-1} \in Z(G)$.
  Let $x\ inG$. Then

  $$ax = xa \implies axa^{-1} = xaa^{-1} = x \implies a^{-1}axa^{-1} = a^{-1}x \implies xa^{-1} = a^{-1}x.$$

  Thus a^{-1} commutes with x for all $x \in G$ and $a^{-1} \in Z(G)$.

We conclude that $Z(G)$ is a subgroup of G. □

Exercise: Show that $Z(D_6)$ is the trivial subgroup.

The centre of a group is the set of elements that commute with *everything*. Another thing that we can do in thinking about pairs of commuting elements is choose a particular element and look at everything that commutes with that.

Definition 2.2.4. *Let* g *be an element of a group* G*. Then the* centralizer *of* g *in* G*, denoted* $C_G(g)$*, is defined to be the set of all elements of* G *that commute with* g*, i.e.*

$$C_G(g) = \{x \in G : xg = gx\}.$$

Please give some care and attention to this definition, and in particular make sure that you understand the distinction between the *centralizer of an element* of a group and the *centre* of a group. The centre of a group consists of all those elements that commute with everything in the group; it is a feature of the group itself. However, centralizers are only defined for particular elements. The centralizer of a particular element g consists of all those elements that commute with g; they don't have to commute with anything else. The centre of the group is the intersection of the centralizers of all elements.

Exercise: Think about the following two problems and write a detailed note on them (the second one is tricky).

1. Let g be an element of a group G. Show that $Z(G) \subseteq C_G(g)$ (i.e. show that the centralizer of g always contains the centre of G).
2. Could it happen for some element G that $C_G(g) = Z(G)$?

Example 2.2.5. *Let* $G = D_8$*, with elements labelled as in Example 2.2.5. We can write down the centralizers of all elements of* G*. Note that* $Z(G) = \{\mathrm{id}, R_{180}\}$*.*

- $C_G(\mathrm{id}) = G$ - all elements commute with the identity, so its centralizer is the whole group.
- $C_G(R_{180}) = G$ - all elements commute with R_{180}, so its centralizer is the whole group; this element is in the centre of D_8.
- $C_G(R_{90}) = \{\mathrm{id}, R_{90}, R_{180}, R_{270}\}$ - R_{90} commutes with all of the rotations but with none of the reflections.
- $C_G(R_{270}) = \{\mathrm{id}, R_{90}, R_{180}, R_{270}\}$ - R_{270} commutes with all of the rotations but with none of the reflections.
- $C_G(T_L) = \{\mathrm{id}, R_{180}, T_L, T_M\}$ - T_L commutes with itself and with the reflection T_M in the axis that is perpendicular to L, and with the elements of the centre.
- $C_G(T_M) = \{\mathrm{id}, R_{180}, T_L, T_M\}$ - T_M commutes with itself and with the reflection T_L in the axis that is perpendicular to M, and with the elements of the centre.
- $C_G(T_N) = \{\mathrm{id}, R_{180}, T_N, T_P\}$ - T_N commutes with itself and with the reflection T_P in the axis that is perpendicular to N, and with the elements of the centre.
- $C_G(T_P) = \{\mathrm{id}, R_{180}, T_N, T_P\}$ - T_P commutes with itself and with the reflection T_N in the axis that is perpendicular to P, and with the elements of the centre.

Theorem 2.2.6. *For every* $g \in G$*,* $C_G(g)$ *is a subgroup of* G*.*

The proof of Theorem 2.2.8 is a problem on Problem Sheet 2.

Two observations about centralizers (related to the exercise above):

1. The centralizer of g in G is equal to G if and only if $g \in Z(G)$.
2. For an element g of G that is not in the centre, $C_G(g)$ will be a subgroup that contains both $Z(G)$ and g (and so properly contains $Z(G)$) but is not equal to G.

The concept of the centralizer can be thought of as measuring how far away an element is from being in the centre of a group. An element is in the centre if its centralizer is the whole group. An element that commutes with many things has a large centralizer, and an element that commutes with relatively few things has a small centralizer. So the order of the centralizer of g is high if g commutes with many things, and low if g commutes with few things. Another way to say this is that the *index* of the centralizer of g is low if g commutes with many things, and high if g commutes with few things (remember that the index of a subgroup H in G is $\frac{|G|}{|H|}$.

The index of the centralizer of an element has an other interpretation.

Definition 2.2.7. *Let G be a group and let $g \in G$. A* conjugate *of g in G is an element of the form xgx^{-1} for some $x \in G$. The set of* all *conjugates of g in G is called the* conjugacy class *of the element g.*

It may not be immediately obvious why this notion of conjugacy is an important one, although there is one context in which it is familiar, namely in general linear groups.

Example 2.2.8. *In $\mathrm{GL}(3,\mathbb{R})$ every element may be interpreted as an invertible linear transformation of $\mathbb{R}^3$, subject to a choice of basis of $\mathbb{R}^3$. Two matrices A and B represent the same linear transformation with respect to different choices of basis if and only if there exists a matrix $P \in \mathrm{GL}(3,\mathbb{R})$ for which*

$$B = PAP^{-1}.$$

This is saying that two matrices in $\mathrm{GL}(3,\mathbb{R})$ represent the same linear transformation (with respect to different bases) if and only if they are conjugates of each other in $\mathrm{GL}(3,\mathbb{R})$, or belong to the same conjugacy class*. Recall that the relationship of conjugacy for matrices is referred to as* similarity*.*

It is not necessarily true in abstract groups that elements which are conjugate to each other will share some concrete property as they do in $\mathrm{GL}(3,\mathbb{R})$. However it is always true that elements that are conjugates of each other have many properties in common. To get a sense of what the definition means we will start with a few observations which might explain the connection to pairs of commuting elements, centralizers etc.

1. Think of the element g as being fixed and imagine that we are looking at the various conjugates of g. These are the elements xgx^{-1} where $x \in G$. The element xgx^{-1} is equal to g if and only if $gx = xg$, i.e. if and only if x commutes with g.

2. This means that if every element of G commutes with g (i.e. if $g \in Z(G)$), then all the conjugates of g are equal to g, and the conjugacy class of g consists only of the single element g.

3. In particular this means that if G is abelian, then every conjugacy class in G consists of a single element (this is not really an interesting case for the concept of conjugacy).

4. So (roughly) the number of distinct conjugates of an element G measures how far away it is from being in the centre. If an element has few conjugates then it commutes with many elements of the group. If an element has many conjugates, it commutes with few elements. We will make this precise later.

5. Every element g of G is conjugate to itself, since for example $g = ggg^{-1}$.

Example 2.2.9. *Let the elements of D_8, the group of symmetries of the square, be denoted by* id, R_{90}, R_{180}, R_{270} *(the rotations), T_L, T_M (the reflections in the perpendicular bisectors of the sides), and T_N, T_P (the reflections in the two diagonals). Then D_8 has five distinct conjugacy classes as follows:*

$$\{\mathrm{id}\},\ \{R_{180}\},\ \{R_{90}, R_{270}\},\ \{T_L, T_M\},\ \{T_N, T_P\}.$$

This is saying that:

- $\{\mathrm{id}\}$ and R_{180} are in the centre.

- R_{90} and R_{270} are conjugate to each other. To confirm this, look at (for example) the element $T_L \circ R_{90} \circ T_L^{-1}$ and confirm that it is equal to R_{270}. You can replace T_L with any of the reflections here, they will all work.

- The reflections T_L and T_M are conjugate to each other. To confirm this you could look at $T_N \circ T_M \circ T_N^{-1}$.
- The reflections T_N and T_P in the diagonals are conjugate to each other. To confirm this you could look at $T_M \circ T_N \circ T_M^{-1}$.

Note that in this case the whole group is the union of the distinct conjugacy classes, and that different conjugacy classes do not intersect each other. This is a general and important feature of groups. We will not prove it formally although you are encouraged (as an exercise) to adapt the following description to a formal proof. If two elements of G are conjugate to each other, then any element that is conjugate to either of them is conjugate to both. Thus the conjugacy class of an element g is the same as the conjugacy class of hgh^{-1} for any $h \in G$. On the other hand, if two elements are not conjugate to each other, then no element can be simultaneously conjugate to both of them, and their conjugacy classes do not intersect.

In the case of D_8 above, we can notice that the numbers of elements in the conjugacy classes (1,1,2,2 and 2) are all factors of the group order which is 8. We will finish Chapter 2 now by showing that this is not an accident.

The following theorem relates the centralizer of an element g of G to the conjugacy class of g. It is a special case of the famous Orbit-Stabilizer Theorem concerning group actions.

Theorem 2.2.10. *Let g be an element of a finite group G. Then the number of distinct conjugates of g is $[G : C_G(x)]$, the index in G of $C_G(g)$.*

Note: Using Examples 2.2.5 and 2.2.7 above, we can verify this theorem for the dihedral group D_8.

It is convenient to mention the following necessary Lemma first, rather than trying to prove it in the middle of the proof of Theorem 2.2.9.

Lemma 2.2.11. *Suppose that H is a subgroup of a finite group G. Let x, y be elements of G. Then the cosets xH and yH are equal if and only if the element $y^{-1}x$ belongs to H.*

Proof. From Lemma 2.1.5 we know that xH and yH are equal if and only if $x \in yH$ (since in this case x belongs to both xH and yH and the cosets are equal since they intersect). This occurs if and only if $x = yh$ for some $h \in H$, i.e., if and only if the element $y^{-1}x$ belongs to H. □

Proof. (of Theorem 2.2.9) Recall that $[G : C_G(x)]$ is the number of left cosets of $C_G(g)$ in G. We will show that two elements of G determine distinct conjugates of g if and only if they belong to distinct left cosets of $C_G(g)$. To see this let x_1 and x_2 be elements of G. Then

$$\begin{array}{rcl} x_1 g x_1^{-1} & = & x_2 g x_2^{-1} \\ \iff g x_1^{-1} & = & x_1^{-1} x_2 g x_2^{-1} \\ \iff g x_1^{-1} x_2 & = & x_1^{-1} x_2 g \\ \iff x_1^{-1} x_2 & \in & C_G(g) \end{array}$$

By Lemma 2.2.10, this occurs if and only if the cosets $x_1 C_G(g)$ and $x_2 C_G(g)$ are equal. Thus elements of G determine distinct conjugates of g if and only if they belong to distinct left cosets of $C_G(g)$, and the number of distinct conjugates of g is the number of distinct left cosets of $C_G(g)$ in G, which is $[G : C_G(g)]$. □

In particular, since $|G| = |C_G(g)|\,[G : C_G(g)]$, the number of elements in each conjugacy class of G is a factor of G. This fact can be used to prove the following important theorem about finite p-groups. A finite p-group is a group whose order is a power of a prime p (e.g. a group of order 27, 64, or 125).

Theorem 2.2.12. *Suppose that G is a finite p-group. Then the centre of G cannot be trivial, i.e. it cannot consist only of the identity element.*

Proof. As an example, suppose that $p = 5$ and that $|G| = 5^4 = 625$. (As an exercise you could adapt the proof for this example to a general proof). Suppose that the conjugacy classes of G are $C_1,\ C_2, \ldots, C_k$. Remember that every element of the centre comprises a conjugacy class all on its own, and that each non-central element belongs to a conjugacy classes whose number of elements is greater than 1 and is a divisor of 5^4. Suppose that C_1 is the conjugacy class that consists only of the identity element. Then

$$|G| = 5^4 = 1 + |C_2| + |C_3| + \cdots + |C_k|.$$

(This is called the *class equation* of G). Each $|C_i|$ is either 1 or a multiple of 5. If all of $|C_2|, |C_3|, \ldots, |C_k|$ are multiples of 5, it means that $|G| = 1 +$ (a multiple of 5), so $|G|$ would have remainder 1 on division by 5. This is not possible since $|G| = 5^4$, so it must be that some (at least 4) of the C_i (apart from C_1) consist of a single element. These "single element" conjugacy classes correspond to non-identity elements of the centre of G. □