2. Orders and classes

From now on, attention will be focused on finite groups (groups containing a finite number of elements), until further notice.

The *order* of a finite group $\mathcal{G}$ is the number of elements it contains and is denoted $|\mathcal{G}|$. Suppose a certain group $\mathcal{G}$ contains an element A, $A \in \mathcal{G}$. Then, by closure, it must also contain any power A^n of A. But $\mathcal{G}$ has a finite number of elements, so not all powers of A can be distinct. There must be some powers k, l such that $A^k = A^l$. Let $k > l$, then $A^{k-l} = A^0 = E$, where $k - l$ is a positive integer. The smallest positive integer r such that $A^r = E$ is called the *order* of A. Each element $A \in \mathcal{G}$ has a well-defined order, which cannot exceed $|\mathcal{G}|$, since the number of distinct powers of A which are contained in $\mathcal{G}$ is equal to the order of A. Only the identity E has order one; all other elements have orders greater than one.

Suppose $A \in \mathcal{G}$ is of order r, i.e. $A^r = E$ and this does not hold for any positive power of A less than r. Then $A^{r-1}A = E$, so that $A^{r-1} = A^{-1}$. Then $A^{r-2} = A^{r-1}A^{-1} = A^{-2}$, so that $A^{r-m} = A^{-m} = (A^{-1})^m$. It follows that $(A^{-1})^r = E$ and r is the smallest positive integer for which this holds.

[If $(A^{-1})^m = E$ for some $m < r$, then $A^{r-m} = E$ with $r - m < r$, a contradiction.]

The order of A^{-1} is the same as the order of A.

Let $A \in \mathcal{G}$ be an element of order $r \leq |\mathcal{G}|$. By closure, $\mathcal{G}$ contains r distinct powers of A, namely A^m with $m = 1, 2, \ldots, r$ and $A^r = E$. This set of r elements (including A itself), with the same associative multiplication rule as $\mathcal{G}$, is closed under multiplication, contains the identity E and also contains the inverse A^{r-m} of each element A^m. It is therefore a group, called the *cyclic group of order* r and denoted $\mathcal{C}_r$. Every element, of order r, of a group generates a cyclic group $\mathcal{C}_r$. The cyclic group $\mathcal{C}_r$ is Abelian and its multiplication table can be written in a form in which each row is a cyclic permutation of the preceding row. The first two groups of order six given as examples earlier were cyclic groups of order six, C_6. A group $\mathcal{G}$ is cyclic if and only if it contains an element of order $|\mathcal{G}|$.

Although there is no limit on the number of different concrete realisations of a given abstract group structure, all isomorphic to one another, there is only a finite number of distinct abstract groups of a given finite order. For the lowest orders, the reasoning is as follows.

$|\mathcal{G}| = 1$: There is a single element, necessarily the identity. The multiplication rule is $EE = E$. There is only one group of order 1, called the

unit group.

$|\mathcal{G}| = 2$**:** There are two elements, the identity E and an element A. By definition, $EE = E$, $EA = A$ and $AE = A$. It remains only to specify AA, the two possibilities being $AA = E$ and $AA = A$. But $AA = A \Longrightarrow A = E$, which is unacceptable, so necessarily $AA = E$. The element A is of order 2. The only group of order 2 is therefore the cyclic group $\mathcal{C}_2$.

$|\mathcal{G}| = 3$**:** There are three elements, the identity E and two other distinct elements A and B. Of the nine products, five involve E and are trivial. There remain AA, AB, BA and BB. As before, $AA = A$ and $BB = B$ are ruled out, as are $AB = A$, $AB = B$, $BA = A$ and $BA = B$, since all would imply either $A = E$ or $B = E$. There remain as sole options $AB = E$ and $BA = E$. Since each row of the multiplication table must be a permutation of E, A, B, it necessarily follows that $AA = B$ and $BB = A$. These results imply that both A and B are of order 3, and that $B = A^2$ and $A = B^2$. The only group of order 3 is the cyclic group $\mathcal{C}_3$, generated either by A or by B.

Tabulations exist of all finite groups of low orders. For $|\mathcal{G}| \geq 4$ there are generally several different groups of each order. A table of finite groups of order up to 31 is listed in the appendix to this chapter.

Given some element $A \in \mathcal{G}$, the distinct elements of the form BAB^{-1}, for all $B \in \mathcal{G}$, are called *conjugate elements* of A and constitute a *conjugacy class* of $\mathcal{G}$. (For reasons of economy, these will be referred to simply as classes.) The class generated by A in this manner contains A itself [both $EAE^{-1} = A$ and $AAA^{-1} = A$] and clearly contains less than $|\mathcal{G}|$ elements. Every element of a class has the same order as the element generating it.

> [Since $(BAB^{-1})^n = BAB^{-1}BAB^{-1}\cdots BAB^{-1} = BA^nB^{-1}$ and $BA^nB^{-1} = E \Longleftrightarrow A^n = E$.]

If B is in the class generated by A, then the class generated by B is the same as the class generated by A.

> [$B = XAX^{-1}$ for some $X \in \mathcal{G}$. The class generated by B is $\{YBY^{-1}$, for all $Y \in \mathcal{G}\}$=$\{YXAX^{-1}Y^{-1}$, for all $Y \in \mathcal{G}\}$ =$\{(YX)A(YX)^{-1}$, for all $Y \in \mathcal{G}\}$=$\{ZAZ^{-1}$, for all $Z \in \mathcal{G}\}$, by the rearrangement theorem. This is just the class generated by A.]

The identity element E is always in a class by itself. In an Abelian group, each element of the group constitutes a class in itself.

$[BAB^{-1} = ABB^{-1} = A$ for every $A, B \in \mathcal{G}]$.

Suppose there is a binary relation defined amongst elements of a set, denoted by $A \sim B$. It is an *equivalence relation* if it satisfies the three conditions $A \sim A$ (the relation is *reflexive*); $A \sim B \Longrightarrow B \sim A$ (the relation is *symmetric*); and $A \sim B, B \sim C \Longrightarrow A \sim C$, for all elements A, B, C of the set (the relation is *transitive*). $A \sim B$ is read "A is equivalent to B". All elements equivalent to a given element A of the set constitute the *equivalence class* of A.

Let A be an element of the set $\mathcal{S}$ in which an equivalence relation is defined and form its equivalence class. In general, this will be a subset of $\mathcal{S}$. Select an element $B \in \mathcal{S}$ which is not in the equivalence class of A and form its equivalence class. The equivalence classes of A and B are completely distinct. [If they had an element C in common, $A \sim C$ and $B \sim C$, then $B \sim A$, a contradiction.] If $C \in \mathcal{S}$ is not in the equivalence classes of A or B, then its equivalence class is entirely distinct from the previous two. Proceeding in this way, the equivalence relation *partitions* the set $\mathcal{S}$ into distinct, non-overlapping equivalence classes.

In the context of groups, being conjugate elements is an equivalence relation.

> [Every element is conjugate to itself, $EAE^{-1} = A$. If B is conjugate to A, there is an X such that $XAX^{-1} = B$. But this implies $X^{-1}BX = A$, so A is conjugate to B. If A is conjugate to B and B is conjugate to C, there exist X and Y such that $XBX^{-1} = A$ and $YCY^{-1} = B$. But then $XYCY^{-1}X^{-1} = A$, or $(XY)C(XY)^{-1} = A$ and A is conjugate to C.]

So the conjugacy classes of a group are equivalence classes and the group is partitioned into distinct, non-overlapping conjugacy classes.

It is sometimes convenient to introduce a structure called the *group algebra*. This is a linear vector space, spanned by the elements of the group, in which the product of two vectors is defined by the group multiplication, assumed distributive. A typical element of the group algebra might be $aX+bY$, where X and Y are elements of the group and a and b are members of the number field over which the vector space is defined. The product of two such elements would be $(aX + bY)(cV + dW) = acXV + bcYV + adXW + bdYW$, where X, Y, V, W are elements of the group, as are the group products

XV, YV, XW, YW, and a, b, c, d are numbers, as are the number products ac, bc, ad, bd. The product is itself an element of the group algebra.

Let the element $A \in \mathcal{G}$ generate a class $\{B_i\}$. Consider the element of the group algebra defined by $\mathcal{C} = \sum_i B_i$. Then $X\mathcal{C}X^{-1}$, for any $X \in \mathcal{G}$, is the same operator $\mathcal{C}$ again, since XB_iX^{-1} is an element of the class and $XB_iX^{-1} = XB_jX^{-1} \Longrightarrow B_i = B_j$. So $X\mathcal{C}X^{-1} = \mathcal{C}$, or $X\mathcal{C} = \mathcal{C}X$, for every $X \in \mathcal{G}$. For every class, the corresponding *class operator* $\mathcal{C}$ can be defined in the group algebra, and it commutes with every element of the group.

Examples

Some examples have been given of groups of order 6. The first two were different realisations of the cyclic group of order 6, $C_6 = \{E, A, A^2, A^3, A^4, A^5\}$, with $A^6 = E$. The element E is of order 1, the element A^3 is of order 2, the elements A^2, A^4 are of order 3 and the elements A, A^5 are of order 6. Since the group is Abelian, each of its 6 elements is in itself a class.

The other two groups presented were also different realisations of a single abstract group. Everything stated here about the group of symmetries of the equilateral triangle can be applied immediately to the group of permutations of three objects, using the isomorphism spelled out previously. The identity element 1 is of order 1 and is itself a class. The elements m_1, m_2, m_3 are all of order 2 and the elements r_1, r_2 are of order 3. It is straightforward to check, with the aid of the multiplication table, that $\{r_1, r_2\}$ constitutes a class, as does $\{m_1, m_2, m_3\}$. This group has three classes. (The fact that in this group all the elements of a given order belong to the same class is consistent with the requirement that all members of a class have the same order, but it is not true of all groups. The group considered is small and this simply happens to be true here.)

Appendix – table of finite groups up to order 31

There is no rule to determine the number of distinct finite groups of a given order (except that there is only one group of each prime order g, namely the Abelian cyclic group $\mathcal{C}_g$). Each order g must be separately investigated. The following table lists the number of groups (Abelian or non-Abelian) of orders 1 through 31.

order	Abelian	non-Abelian	total
1	1	0	1
2	1	0	1
3	1	0	1
4	2	0	2
5	1	0	1
6	1	1	2
7	1	0	1
8	3	2	5
9	2	0	2
10	1	1	2
11	1	0	1
12	2	3	5
13	1	0	1
14	1	1	2
15	1	0	1
16	5	9	14
17	1	0	1
18	2	3	5
19	1	0	1
20	2	3	5
21	1	1	2
22	1	1	2
23	1	0	1
24	3	12	15
25	2	0	2
26	1	1	2
27	3	2	5
28	2	2	4
29	1	0	1
30	1	3	4
31	1	0	1

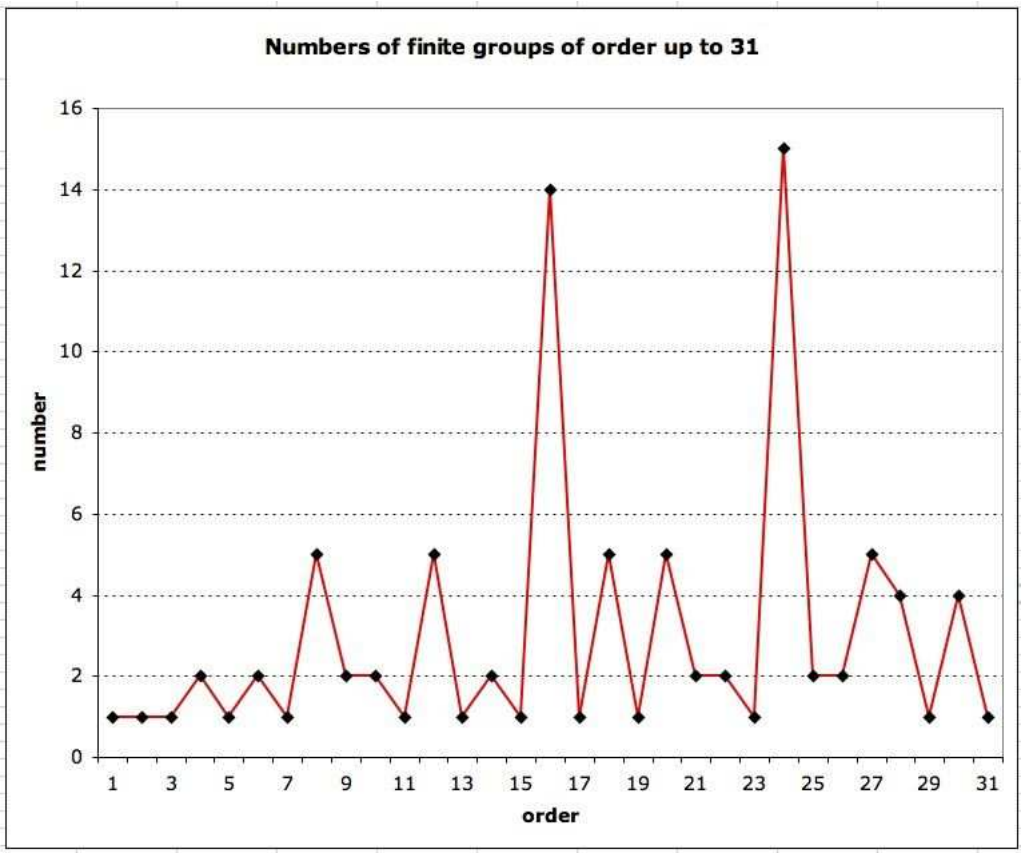

Figure 1: A graphic presentation of the number of finite groups of orders from 1 to 31.