Abel Prize 2008

A short Introduction to Group Theory

The Abel Prize for 2008 is awarded within the subfield of group theory. This note provides a short introduction to the theory. We shall state the main definitions and look at some examples. This is not to be considered as a textbook on the topic, but rather as a guide to the interested reader.

Definition
A **group** is a set G equipped with a binary operation $G \times G \to G$ which two each pair of elements x, y in G assigns a unique third element xy in G, satisfying the following axioms:

1. Associative law: (xy)z=x(yz) for all elements x,y,z in G.
2. Existence of a unit, i.e. an element e in G satisfying xe=ex=x for all x in G.
3. Existence of inverses, i.e. for all x in G, there is another element y in G, called the inverse of x, and satisfying xy=yx=e. We write $y=x^{-1}$.

If in addition the axiom of commutativity is fulfilled the group is **abelian**, named after Niels Henrik Abel:

4. Commutative law: xy=yx for all x,y in G.

For the binary operation of an abelian group we normally use the sign + rather than the product notation. The unit of an abelian group is denoted 0 and for the inverse we use –x rather than x^{-1}.

Example 1
Let G be the set of integers, denoted by $\mathbf{Z}$. In this example the binary operation is ordinary addition; to a pair of numbers we associate the ordinary sum. The unit of $\mathbf{Z}$ is the number 0, and the inverse of x is –x, for any x. Thus the inverse of -2 is -(-2)=2. This is an abelian group since the sum is independent of the order of the terms; 2+5=5+2.

Example 2
The second example is the symmetry group of a square. We number the vertices of the square as follows: $\begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}$. A reflection S about the vertical symmetry axes is written $\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$. A 90-degree clockwise rotation R is given by $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$. Reflecting twice about the same axes gives the identity, formalised by $SS=S^2=e$, Four 90-degree rotations gives a whole circle, i.e. $R^4=e$. The two symmetries R and S generate the whole symmetry group, but there is a relation between them. Reflecting about the horizontal axes is given by $\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$, this symmetry is obtained by performing S and then R twice. The same result is obtained by composing a 90-degree counter clockwise rotation (R^{-1}) and a reflection (S), in that order. The relation is written $SR=R^{-1}S$. This group is called D_4 (*Dihedral group* on 4 vertices).

Example 3
The smallest group is the one with one element, G={e}. It is called the **trivial group.**

When mathematicians define new objects they always look for possible maps between these objects, subobjects and quotients.

Definition
A map $\beta : G \to G'$ between two groups G and G´ is called a **homomorphism** if it preserves the group structure, i.e. maps products to products, units to units, and inverses to inverses. For a technical definition we need only one axiom

$$\beta(xy) = \beta(x)\beta(y)$$

for all x,y in G.

Example 4

We define a homomorphism $\beta: Z \to D_4$ by $\beta(n) = R^n$ for all integers n. It is easy to see that this map satisfy the homomorphism axiom;

$$\beta(n+m) = R^{n+m} = R^n R^m = \beta(n)\beta(m)$$

(It may be confusing that the group operation is written as + in ***Z*** and multiplicatively in D_4). Since R is a 90-degree rotation we see that $\beta(4) = e$ and also that $\beta(n) = e$, for all numbers n, divisible by 4. This set is denoted the **kernel** of the homomorphism. The notion of a kernel is of course general; the kernel of a homomorphism is the subset mapped to the unit by the homomorphism.

Definition

(Weak version): A subset H of a group G is called a **subgroup** of G if H itself is a group under the restricted binary operation, i.e. the operation is closed on H, e is in H, and for any x in H, the inverse x^{-1} is also in H.

(Strong version): A subgroup H of G is called a **normal** subgroup if it is the kernel of any homomorphism from G into some other group.

What is the difference between the two versions? Or better, why do we need two versions? The weak version is the natural definition, and the strong version is the one we use to build arbitrary groups from simple groups.

Definition

A group G is **simpel** if it has no other normal subgroups than the trivial subgroup and the group itself.

The simple groups play the same role in group theory as atoms play in chemistry, as primes in number theory and as points in geometry.

There are no limitations for the order of a group (number of elements of the group). The trivial group has one element and **Z** has an infinite number. It is eight symmetries of a square, and the dihedrale group D_4 has order eight.

This is just the basis of the theory. The more sophisticated part is left to the reader as a self study.