A combinatorial view of groups

Originally, groups were defined as "all symmetries of an object."

To be concrete, we take an "object" to be a pair (X,S) where X is a set (the groundset) and S is a structure defined on X.

Ex: S could be a graph on X
... a partition of X
... a permutation of X

Given any permutation (defined here as bijection) of X, there is a natural way to apply it to an object.

The permutation π of X is an automorphism of (X,S) if

$$\pi(S) = S.$$

The automorphism group of (X,S) is the set $\mathrm{Aut}(X,S)$ of all automorphisms of (X,S).

We will take this as our first definition of a "group"

Every automorphism group satisfies three properties:

① it contains the Identity permutation, trivially,

② it contains the inverse of each of its elements - if $\pi(S)=S$ then $S=\pi^{-1}(S)$,

③ it is closed under composition - if $\pi(S)=S$ and $\sigma(S)=S$, then $\sigma(\pi(S))=S$.

For our second definition of a "group" we are more general. A permutation group is a set G of permutations of some set X which satisfies ①-③.

First though, is this really more general?

Or, is every permutation group an automorphism group? (of some object)

Proposition: Every permutation group is an automorphism group.

Proof: Let G be a permutation group on the set $X=\{x_1,\dots,x_n\}$.

Define $S=\{(\pi(x_1),\dots,\pi(x_n)) : \pi\in G\}$.

Claim: $\mathrm{Aut}(X,S)=G$.

For $\pi \in G$,

$$\pi(S) = \{(\pi(\sigma(x_1)), \dots, \pi(\sigma(x_n))) : \sigma \in G\}$$

By ② and ③,

$$G = \{\tau \circ \pi^{-1} : \tau \in G\},$$

so

$$\pi(S) = \{(\pi(\pi^{-1}(\tau(x_1))), \dots, \pi(\pi^{-1}(\tau(x_n))) : \tau \in G\}$$
$$= \{(\tau(x_1), \dots, \tau(x_n) : \tau \in G\}$$
$$= S,$$

so $G \le \mathrm{Aut}(X, S)$.

Now consider some $\pi \in \mathrm{Aut}(X,S)$. By ①, G contains the identity, so S contains $(x_1, \dots, x_n)$. The action of π on S sends this tuple to $(\pi(x_1), \dots, \pi(x_n))$, so $\pi \in G$, proving $\mathrm{Aut}(X,S) \le G$. ■

In the late 1800s, Dyck defined an <u>abstract group</u> as a set G with an operation $\cdot$ that satisfies

ⓐ associativity:

$$g \cdot (h \cdot k) = (g \cdot h) \cdot k$$

ⓑ identity:

$$\exists e \in G \text{ such that } e \cdot g = g \cdot e = g$$

ⓒ inverses:

$$\forall g \in G\ \exists g^{-1} \in G \text{ such that}$$
$$g \cdot g^{-1} = g^{-1} \cdot g = e.$$

This was not well-received.

Klein: "the disadvantage of the abstract method is that it fails to encourage thought."

Is this definition any more general?

No:

<u>Cayley's Theorem</u>: Every abstract group is isomorphic to a permutation group.

<u>Proof</u>: Let G be an abstract group. We want to find an isomorphic permutation group on some set X.

Let $X = G$, and $G' = \{\rho_g : g \in G\}$ where

$$\rho_g(x) = g \cdot x$$

for all $x \in X$ $(= G)$.

Because G has an identity element e, if $g \ne h$ then

$$\rho_g(e) = g \ne h = \rho_h(e),$$

so

$$\rho_g \ne \rho_h.$$

We also have

$$(\rho_g \circ \rho_h)(x) = \rho_g(\rho_h(x))$$
$$= \rho_g(h \cdot x)$$
$$= g \cdot (h \cdot x)$$
$$= (g \cdot h) \cdot x$$
$$= \rho_{g \cdot h}(x).$$

Verifying the permutation group axioms ①-③ for G' is easy, and thus $G \cong G'$, a permutation group. ■

Recall that if N is a normal subgroup of G, then G can be broken into two groups:

N and G/N, the quotient group.

If we start with a finite group, we can continue this breaking process until we end up with a collection of *simple groups* (groups without normal subgroups).

The Jordan-Hölder Theorem says that the set of simple groups we end up with is unique.

Therefore, we really only care about the finite simple groups.

These have been classified into 18 infinite families and 26 exceptions, called *sporadic groups*.

The first of these to be found were the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, and M_{24}, reported in his papers from 1861 to 1873.

Until 1960, no others were found...

In the 1960s, work on the characterization took off, and indicated that other sporadic groups might exist.

In general, the number of elements and their orders would be known, but one needed to actually construct the group to prove that it existed.

These were mostly constructed as automorphism groups of graphs.

Higman-Sims group HS

44,352,000 elements

Constructed in 1967 as, essentially, the automorphism group of a

22-regular (every vertex has degree 22) graph with
100 vertices,
and thus...
1100 edges.

The graph is actually the unique graph with these parameters such that

- it does not contain K_3, and
- every pair of non-neighboring vertices share precisely 6 common neighbors.

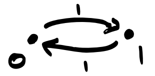
Are all finite groups isomorphic to automorphism groups of graphs?

Frucht's Theorem: Yes.

We sketch a proof. First, we define Cayley digraphs.

Suppose G is a group and $S \subseteq G \setminus \{e\}$. The Cayley digraph $D(G,S)$ has vertices G, and for each $g \in G$ and $s \in S$, there is an edge from g to $g \cdot s$ Labeled by s.

Ex: $G = \mathbb{Z}_2$, $S = \{1\}$,

$D(G,S)$: 

Facts: ① $D(G,S)$ is connected if and only if S generates G (i.e., every element of G is a product of elements of S)

② For each $g \in G$, the map
$$\rho_g : x \mapsto g \cdot x$$
is an automorphism of $D(G,S)$.

③ The automorphisms of G which preserve edge Labels are precisely the automorphisms of ②. Therefore these automorphisms form a group isomorphic to G.

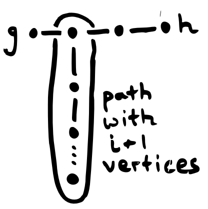
Proof: Exercise.

Sketch of Frucht's Theorem proof:

Take G to be a group with m elements, and set
$$S = G \setminus \{e\} = \{s_1, \dots, s_{m-1}\}.$$
We know that G is isomorphic to the automorphisms of $D(G,S)$ which preserve edge labels.

How can we build an undirected graph with precisely these automorphisms?

Repace $g \xrightarrow{s_i} h$ by the "gadget"


g
h
path with i+1 vertices