Classification of finite groups

A main goal of group theory is the *classification of groups*. That is, we would like to understand what all the possible groups are. If we can achieve this goal, then we understand all groups! Let us focus today on the case of *finite* groups.

When finding all possible finite groups, we want to avoid duplicates. For example, we know that the symmetric group S_3 is isomorphic to the group of symmetries of an equilateral triangle. As another example, we know $\mathbb{Z}_{10}^\times$ is isomorphic to $\mathbb{Z}_4$. We only want to list one such group for each isomorphism type. So we only write S_3 and $\mathbb{Z}_4$ for the above examples, and forget about the others, because they are isomorphic to one of these groups.

Thus our goal is narrowed down to the classification of finite groups *up to isomorphism*. Below is a table which classifies groups up to isomorphism up to order 14.

Order	Groups
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, S_3
7	$\mathbb{Z}_7$

Order	Groups
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q_8
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_5
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, A_4, D_6, T
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_7

Let us explain some of what is in this table. Recall we proved that every group of prime order is cyclic, and further that every finite cyclic group is isomorphic to some $\mathbb{Z}_n$. This covers the cases $2, 3, 5, 7, 11, 13$ in the table.

Let G be a group of order 4. Suppose G is not cyclic, i.e. $G \ncong \mathbb{Z}_4$. Let $a, b \in G$ be distinct non-identity elements. Then ab must have order dividing $|G| = 4$. We cannot have $\text{ord}(ab) = 4$ for otherwise G is cyclic. Suppose $\text{ord}(ab) = 1$. Then $ab = e$, or $a = b^{-1}$, and $b^2 = e$ implies $a = b^{-1} = b$, contradiction. Thus $\text{ord}(ab) = 2$. Further, ab is distinct from a, b. To see this, note that if $ab = a$ then $b = e$, and if $ab = b$ then $a = e$. We may thus write

$$G = \{e, a, b, ab\}$$

Further, $(ab)^2 = abab = e = a^2b^2$ implies $ba = ab$. This determines the group operation on all elements of G, and in particular the Cayley table for G. Now we define a map

$$\phi : G \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$$

by setting $\phi(e) = 0$, $\phi(a) = (1,0)$, $\phi(b) = (0,1)$ and $\phi(ab) = (1,1)$. It is straightforward to verify that ϕ is an isomorphism. Thus we have shown that a group of order 4 which is not isomorphic to $\mathbb{Z}_4$ is in fact isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

You have seen most of the groups in the above table: the exceptions are perhaps D_n and T. The group D_n is the *Dihedral group* of order $2n$, and for $n \geqslant 3$ is non-abelian. It can be defined as the symmetries of a regular n-gon in the plane.

The group T of order 12 may be described in quaternion notation as follows:

$$T = \Big\{1,\ -1,\ \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}\mathbf{i},\ -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}\mathbf{i},\ -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}\mathbf{i},\ \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}\mathbf{i},$$
$$\mathbf{j},\ -\mathbf{j},\ \tfrac{1}{2}\mathbf{j} + \tfrac{\sqrt{3}}{2}\mathbf{k},\ -\tfrac{1}{2}\mathbf{j} + \tfrac{\sqrt{3}}{2}\mathbf{k},\ -\tfrac{1}{2}\mathbf{j} - \tfrac{\sqrt{3}}{2}\mathbf{k},\ \tfrac{1}{2}\mathbf{j} - \tfrac{\sqrt{3}}{2}\mathbf{k}\Big\}$$

As in the quaterion group Q_8, the quaternions $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ satisfy $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, and $\mathbf{ij} = \mathbf{k}$.

You can continue with the brute force reasoning we used above for $|G| = 4$ and show that every non-abelian group of order 6 is isomorphic to S_3. But continuing in this fashion will only get you so far.

The first measure we can take to narrow our scope is to separate the abelian and non-abelian finite groups. The non-abelian entries in the above table are in red. Classifying finite *abelian* groups is a problem that can be solved, and the answer is rather simple:

▸ **Classification of finite abelian groups: Any finite abelian group is isomorphic to a product of cyclic groups of the following form, where the p_i's are primes:**

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$$

In this classification, note that the primes p_i need not be distinct. For example, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the case where $n = 2$, $p_1 = p_2 = 2$ and $a_1 = a_2 = 1$.

▸ **Example:** Consider the group $\mathbb{Z}_{24}^\times$. This is a finite abelian group, so it must be isomorphic to a group as described above. We first write out

$$\mathbb{Z}_{24}^\times = \{1, 5, 7, 11, 13, 17, 19, 23\}$$

where each integer is understood $\pmod{24}$. Thus $|\mathbb{Z}_{24}^\times| = 8$ and so by the Classification Theorem of finite abelian groups, $\mathbb{Z}_{24}^\times$ must be isomorphic to one of

$$\mathbb{Z}_8 = \mathbb{Z}_{2^3} \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_2 = \mathbb{Z}_4 \times \mathbb{Z}_2 \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Note that $5^2 \equiv 25 \equiv 1 \pmod{24}$, $7^2 \equiv 49 \equiv 1 \pmod{24}$, and so on – every element of $\mathbb{Z}_{24}^\times$ apart from the identity has order 2. The only of the above 3 groups that shares this property is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. We conclude that $\mathbb{Z}_{24}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

After classifying abelian finite groups, we may restrict our attention to *non-abelian* finite groups. Another way to narrow our scope is to focus only on *simple* groups.

▸ **A group G is *simple* if $G \neq \{e\}$ and its only normal subgroups are $\{e\}$ and G.**

Finite simple groups are thought of as the "building blocks" for all finite groups. If a finite group G is *not* simple, it has a non-trivial proper normal subgroup $N \subset G$. We obtain an onto homomorphism $G \to G/N$ to a *smaller* group G/N. Then G is to be thought of as decomposed into the smaller parts of N and G/N. If on the other hand G is simple, there is no homomorphism to a smaller non-trivial group, and G cannot be "decomposed".

▸ **Classification of finite simple groups: A finite simple group is isomorphic to:**

(1) A cyclic group $\mathbb{Z}_p$ of prime order.

(2) An alternating group A_n where $n \geqslant 5$.

(3) A finite non-abelian group of "Lie Type".

(4) A "Sporadic" finite non-abelian group, of which there are 26.

This classification theorem is one of the most important results in the history of mathematics. Its proof originally rested on tens of thousands of pages of work due to many mathematicians, although the proof has been simplified over the years. The classification was stated in the 1980's by Gorenstein, although the proof was finished years later.

What are the groups on this list? We know all about the cases (1) $\mathbb{Z}_p$ and (2) A_n. The groups in (3), of "Lie Type", fall into a list of infinite families of systematically constructed groups. To give one family in this type, for each prime p consider:

$$\mathrm{SL}_2(\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a,b,c,d \in \mathbb{Z}_p, \qquad ad - bc \equiv 1 \pmod{p} \right\}$$

This group is generally not simple, because it has a normal subgroup of order 2 consisting of $\{I, -I\}$ where I is the identity matrix (modulo p). However, the quotient group

$$\mathrm{PSL}_2(\mathbb{Z}_p) = \mathrm{SL}_2(\mathbb{Z}_p)/\{I, -I\}$$

is simple when $p \geqslant 5$. In fact, the first few of these are isomorphic to groups you know:

$$\mathrm{PSL}_2(\mathbb{Z}_2) \cong S_3 \qquad \mathrm{PSL}_2(\mathbb{Z}_3) \cong A_4 \qquad \mathrm{PSL}_2(\mathbb{Z}_5) \cong A_5$$

But for higher primes p these are genuinely new groups. Other groups of "Lie type" are of a similar flavor, in a broad sense.

The final category (4) of "Sporadic" finite simple groups are a list of 26 groups that do not follow a systematic pattern. They all have order well over 1000. The largest of these, called the Monster Group, has order about 8×10^{53}, and was constructed by Richard Griess in 1982 as a group of rotational symmetries in 196883-dimensional space.