The Beastiary of Groups

In exploring the natural world, folks in the Middle Ages composed beastiaries, books cataloguing the kinds of animals - real and mythical - that exist. Likewise, in the world of groups we would like to create a beastiary of all the different kinds of groups there are...

U_n, $\mathbb{Z}_n$, S_n, ...

Some groups that look different are really "the same", just like different animals of the same species. For groups, this sameness is called isomorphism.

Ex: U_n is isomorphic to $\mathbb{Z}_n$ $\quad (U_n \cong \mathbb{Z}_n)$

Quest: What are all the groups, up to isomorphism?

This question is HARD. Way, way too hard. Still, we can start our beastiary...

$$\boxed{\text{Pages of the Beastiary Book of } \cancel{\text{Beasts}} \text{ Groups}}$$

- cyclic groups $\mathbb{Z}$, $\mathbb{Z}_n$
  we learned that all cyclic groups are isomorphic to one of these

- symmetric group S_n
  the set of all permutations of $\{1, 2, \ldots, n\}$
  Cayley's Theorem: all finite groups are subgroups

- alternating group $A_n = \{\sigma \in S_n \mid \operatorname{sgn}\sigma = 1\}$
  the subgroup of all even permutations
  = kernel of the sign homomorphism $\operatorname{sgn}: S_n \to U_2$

- dihedral group $D_n = \{e, \rho, \rho^2, \dots, \rho^{n-1}, \mu, \mu\rho, \mu\rho^2, \dots, \mu\rho^{n-1}\}$
  the group of symmetries of a regular n-gon.
  ρ = rotation counter-clockwise by $2\pi/n$ radians
  μ = reflection across the y-axis

We can create more subgroups in many ways.
- subgroups
- direct products (direct sums)
- semi-direct products

...

__Def__: The __direct product__ of two groups G and H is
$G \times H = \{(g,h) \mid g \in G,\ h \in H\}$, $(g_1,h_1)*(g_2,h_2) = (g_1 * g_2, h_1 * h_2)$
if G, H are Abelian and $* = +$ we call this the __direct sum__ $G \oplus H$

In the same way molecules are made up of atoms, we can try to break a group down into products of smaller groups until we get to certain "atoms" which we can break no farther:

$$\mathbb{Z}_{70} \cong \mathbb{Z}_7 \oplus \mathbb{Z}_{10} \cong \mathbb{Z}_7 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5$$

__Def__: A group G is __decomposable__ if $G \cong H \times K$ for some H, K nontrivial. Otherwise it is __indecomposable__.

Refined Quest: Can we find all the indecomposable groups up to isomorphism? Too hard!

What about if we focus on Abelian groups?

Examples: $\mathbb{Q}$ with addition

$\mathbb{T} = \{ z \in \mathbb{C} \mid |z| = 1 \}$ with multiplication

p-adic groups

crazy large groups ...

Still too hard!

So we will focus on finitely generated abelian groups.

Def: A group G is finitely generated if there exist $g_1, g_2, \dots, g_r \in G$ with $G = \langle g_1, \dots, g_r \rangle$.

Ex: $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z} = \langle (1,0), (0,1) \rangle$, so it is finitely generated.

Ex: $\mathbb{Z}_{70}$ is finite so it is finitely generated

Ex: $\mathbb{T}$ is uncountable so it is finitely generated

Ex: $\mathbb{Q}$ is not finitely generated, even though it is still countable.

Quest: What are the indecomposable, finitely generated Abelian groups?

Theorem: $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ if and only if $\gcd(m,n) = 1$

Proof:

S'pose $\gcd(m,n) = r > 1$. Then $r \mid m$ and $r \mid n$ so that for all $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$

$$\frac{mn}{r}(a,b) = \left(\frac{n}{r} ma, \frac{m}{r} nb\right) = \left(\frac{n}{r}0, \frac{m}{r}0\right) = (0,0)$$

However $\frac{mn}{r} \cdot 1 \neq 0$ in $\mathbb{Z}_{mn}$ so if $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ is an isomorphism & $(a,b) = f(1)$

$$(0,0) \neq f\left(\frac{mn}{r}\right) = \frac{mn}{r} f(1) = \frac{mn}{r}(a,b) = (0,0)$$

This is a contradiction.

Now suppose $\gcd(m,n) = 1$.

Define

$$g: \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$$
$$(a,b) \mapsto na + mb$$

It's easy to see this is a homomorphism.

Also since $\gcd(m,n) = 1$ $\exists$ $j,k \in \mathbb{Z}$ with $jm + kn = 1$ and therefore $g(k,j) = 1$ so that $g(\ell k, \ell j) = \ell$

Hence g is surjective and thus bijective because both groups have the same (finite) size

$\square$

Ex: $\mathbb{Z}_{500} = \mathbb{Z}_{125 \cdot 4} \cong \mathbb{Z}_{125} \oplus \mathbb{Z}_4$

Ex: $\mathbb{Z}_{720} = \mathbb{Z}_{5 \cdot 144} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{144}$

$$\cong \mathbb{Z}_5 \oplus \mathbb{Z}_{9 \cdot 16}$$

$$\cong \mathbb{Z}_5 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{16}$$

Corollary: If G is finite, Abelian and indecomposable, $G \cong \mathbb{Z}_{p^n}$ for some prime p.

Q: What about when G is infinite?

Theorem: If G is infinite, Abelian and indecomposable, $G \cong \mathbb{Z}$.

This allows us to completely classify all f.g. Abelian groups!

Structure Theorem for Finitely Gen. Ab. Groups (prime divisor version)

If G is a finitely gen. Abelian group then

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \dots \oplus \mathbb{Z}_{p_d^{r_d}}$$

for some prime numbers $p_1, \dots, p_d \in \mathbb{Z}$ and integers $r \geq 0$ and $r_j > 0$ for $j = 1, \dots, d$.

These are unique up to reordering the primes.

Ex: How many groups of order 27?

$$\mathbb{Z}_{3^3}, \quad \mathbb{Z}_{3^2} \times \mathbb{Z}_3, \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

three!

Sometimes we may prefer this in invariant factor form.

Structure Theorem for Finitely Gen. Ab. Groups (invariant factor form)

If G is a finitely gen. Abelian group then

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \dots \oplus \mathbb{Z}_{a_m}$$

for some integers $r \geq 0$ and $a_1, a_2, \dots, a_m \in \mathbb{Z}$ with $a_1 \mid a_2 \mid \dots \mid a_m$.

This form is unique.

<u>Def</u>: The elements $a_1, \dots, a_m$ are called <u>invariant factors</u>

<u>Ex</u>:

$$\begin{tikzcd}
& \mathbb{Z}_{100} \times \mathbb{Z}_6 \arrow[dl] \arrow[dr] & \\
\mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 & & \mathbb{Z}_2 \times \mathbb{Z}_{300}
\end{tikzcd}$$

prime divisor form

invariant factor form