Math 122 Friday, September 23

<u>defn</u> $\#G$ = <u>order</u> of group = number of elements $g \in G = 1, 2, 3, \ldots$ or ∞

e.g. $\#\{e\} = 1$; $\#\{e, g\} = 2$, $g^2 = e$; $\#(\mathbb{Z}, +) = \infty$

The <u>order</u> of an <u>element</u> $g \in G$ = the order of the subgroup $\langle g \rangle$
$= \{e, g, g^{-1}, g^2, g^{-2}, \ldots\} \subset G$. $g^a \cdot g^b = g^{a+b}$ $a, b \in \mathbb{Z}$

If $g^a = g^b$ for some $a > b$ then $g^{a-b} = e$ for some $n = a-b > 0$. Let n = smallest positive power of g with $g^n = e$.

<u>Claim</u> If n is as above then $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$ has order n.

Note: $g^{-1} = g^{n-1}$ and $g^m = g^{nk+r} = g^{nk} \cdot g^r = e^k \cdot g^r = g^r$ $0 \le r < n$. If $g^a = g^b$ for some $a, b < n$ then $g^{a-b} = e$ and $a - b < n \Rightarrow \Leftarrow$.

If G is finite, so is any subgroup $H \subset G$. So $\langle g \rangle$ is finite for any $g \in G$ so order of g is finite for any $g \in G$.

ex: S_3
- e order 1
- $(12), (23), (13)$ order 2
- $(123), (132)$ order 3

note: 1, 2, and 3 each divide $\#S_3 = 6$
This will be true more generally (proof to follow soon).

<u>Future Thm</u> The order of g always divides $\#G$.

<u>defn</u> G is <u>cyclic</u> if $\exists g \in G$ with $\langle g \rangle = G$

Note: all cyclic groups are ab<u>elian</u>! $g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b g^a$

ex: S_3 not cyclic. $\mathbb{Z}$ is cyclic generated by 1 or -1.

There is a finite group G of <u>order</u> p (a prime) for every prime p, and it is <u>cyclic</u>. Note: existence of a group of order $p \Rightarrow$ cyclic by Future Thm. If $g \in G$ is not e then order of $g > 1$ and divides $p \Rightarrow \#\langle g \rangle = \#G = p$.

ex: An abelian group of order 4 which is <u>not</u> cyclic.

$G = \{e, (12)(34), (13)(24), (14)(23)\} \subset S_4$ All $g \neq e$ have order 2 so don't generate G.

ex: Another group of order 4, not cyclic (but abelian).

$$G' = \left\{ \underset{e}{\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}},\ \underset{g}{\begin{pmatrix} -1 & \\ & 1 \end{pmatrix}},\ \underset{h}{\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}},\ \underset{j}{\begin{pmatrix} -1 & \\ & -1 \end{pmatrix}} \right\} \subset GL_2(\mathbb{R})$$

$$g^2 = e \qquad h^2 = e \qquad j^2 = e$$

How can we compare two groups G and G' which are defined in different ways.

<u>defn</u> A <u>homomorphism</u> of groups $f: G \to G'$ is a map of sets which satisfies $f(\underset{\text{in } G}{g_1 \cdot g_2}) = f(g_1) \underset{\text{in } G'}{\cdot} f(g_2)$. Note this condition implies that $f(e) = e'$ and $f(g^{-1}) = f(g)^{-1}$!

<u>defn</u> An <u>isomorphism</u> is a homomorphism which is a bijection of sets.

ex: There exists an isomorphism $f: G \to G'$ from the two groups defined above
$f(e) = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$, $f((12)(34)) = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$, $f((13)(24)) = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$, $f((14)(23)) = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$

Note: if two groups are isomorphic (written $G \simeq G'$) then they have the same number of elements of each order. If g has order n in G and f is an isomorphism then $f(g) = g'$ has order n in G'.

More non-abelian groups.

Recall if G has prime order it is cyclic $\Rightarrow$ abelian by Future Thm and we'll show that G of order p^2 also abelian.

So smallest non-abelian group has order 6 (e.g. S_3). Next smallest of order 8.

ex: non-abelian of order 8 $\{\pm 1, \pm i, \pm j, \pm k\}$ $(-1)^2 = 1$ $i^2 = (-i)^2 = j^2 = (-j)^2 = k^2 = (-k)^2 = -1$
$ijk = -1$, $ij = -k^{-1} = -(-k) = k$, $ji = -k$, $k^3 = k k^2 = k(-1) = -k$, $k^4 = e$

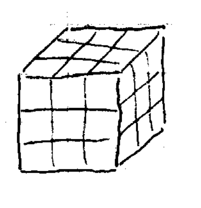
Called the Hamilton quaternions after Irish mathematician Hamilton who struggled to define a multiplication law on a real vector space of dimension 3 and found one of dimension 4.

$$\mathbb{R} \subset \underset{2}{\mathbb{C}} \subset \underset{4}{\mathbb{H}} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

Other non-abelian examples:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

puzzle and the Rubik's cube



The group G of permutations of the Rubik's cube can be thought of as a subgroup of S_{26} (the center stays fixed). In fact:

$$G \subset \underset{\text{centers}}{S_6} \times \underset{\text{corners}}{S_8} \times \underset{\text{edges}}{S_{12}}$$

In fact centers stay fixed so $g \in G$ is $g = (e) \times \text{perm in } S_8 \times \text{perm in } S_{12}$

More precisely $h = e \times (abcd) \times (a'b'c'd')$. We'll see that not all permutations in $S_8 \times S_{12}$ are possible.

Problem of "solving the cube" is taking a permutation that is possible and then finding the shortest sequence of generating moves to express that permutation.

Note Rubik's group $\#G \,|\, 8!\,12!$ is really not that big.

For the Monster group $\#G \sim 10^{47}$