Math 122 Friday, November 4

Classification of G using $\#G$

$\#G = p$ then G is cyclic, any $g \neq e$ is a generator $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} G$ $a \mapsto g^a$

$\#G = p^2$ then G is abelian (because center is non-trivial, so G/Z either trivial $\Rightarrow G$ abelian or cyclic $\Rightarrow G$ abelian by midterm)
If $\exists\, g \in G$ of order p^2 then $\mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\sim} G$ $a \mapsto g^a$
If not, all elements $g \neq e$ have order p so $\mathbb{Z}/p\mathbb{Z}$ acts by scalars on G $a \cdot g = g^a$.
So G is a vector space over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $\dim = 2$ so choose a basis $G \cong \mathbb{Z}/p\mathbb{Z} + \mathbb{Z}/p\mathbb{Z}$.

$\#G = pq$ p,q primes $p < q$. We'll use the Sylow Thms

Thm (Sylow) If $p^n \| \#G$ (note "$\|$" means "exactly divides", i.e. $p^{n+1} \nmid \#G$) then $\exists\, H \subset G$ of order p^n and all such H are conjugate. N divides $[G:H]$ and $N \equiv 1 \pmod p$
Note $N = 1 \iff H \trianglelefteq G$ (where N = number of Sylow-p subgroups).

Assume first that $q \not\equiv 1 \pmod p$. Then both $H_p \trianglelefteq G$ of index q and $H_q \trianglelefteq G$ of index p. (note $p < q \Rightarrow p \neq 1 \pmod q \Rightarrow$ Sylow-q subgroup is always normal).

So any g of order p lies in $H_p \Rightarrow$ there are $p-1$ elements of order p in G.
any g of order q lies in $H_q \Rightarrow$ there are $q-1$ elements of order q in G.
e has order 1 $\Rightarrow$ $1 + (p-1) + (q-1)$ elements have order $< pq \Rightarrow$
$pq - (p-1) - (q-1) - 1 = pq - p - q + 1 = (p-1)(q-1) > 0$ elements have order pq
Hence if g has order pq then $\mathbb{Z}/pq\mathbb{Z} \xrightarrow{\sim} G$ $a \mapsto g^a$.

If $q \equiv 1 \pmod p$ then we can have either 1 or q Sylow-p subgroups H_p.
If $N = 1$ then $G \cong \mathbb{Z}/pq\mathbb{Z}$ by the above argument.
If $N = q$ then G is non-abelian as H_p is not normal.
Have $q \cdot (p-1)$ elements of order p, $q-1$ elements of order q, and the identity
$q(p-1) + (q-1) + 1 = pq$.

ex. D_q of order $2q$. Has $q-1$ rotations of order q and q reflections of order 2.

In general can build G from a normal subgroup.
$\langle 1, g, g^2, \ldots, g^{q-1} \rangle = H_q \trianglelefteq G$
$\langle 1, h, h^2, \ldots, h^{p-1} \rangle = H_p \subset G$ Every $\in G$ can be expressed in the form $g^a h^b$. $a \in \mathbb{Z}/q\mathbb{Z}$ $b \in \mathbb{Z}/p\mathbb{Z}$

If $g^a h^b \equiv g^{a'} h^{b'}$ then $g^{a-a'} = h^{b'-b} = e \Rightarrow a \equiv a' \pmod q$, $b \equiv b' \pmod p \Rightarrow$ expression is unique!
(as $H_p \cap H_q = \{e\}$)

Must give a formula for commutation of g: $hgh^{-1} = g^a$ (in H_q as $H_q \triangleleft G$)

For D_q, $H_2 = \langle 1, h \rangle$. $hgh^{-1} = g^{-1}$ for dihedral group, $a \equiv -1 \bmod q$.
$a = 1$ gives $G = \mathbb{Z}/pq\mathbb{Z}$, $a = 1$ gives $G = D_q$. $hgh^{-1} = g^a$

Say we did not know this already. $hgh^{-1} = g^a$. We'll use the fact that h has order p and that $(hgh^{-1})^k = hg^k h^{-1}$. So $g = h^p g h^{-p} = h^{p-1} g^a h^{-(p-1)} = h^{p-2}(hg^a h^{-1})h^{-(p-2)} = h^{p-2}(hgh^{-1})^a h^{-(p-2)}$
$= h^{p-2}(g^a)^a h^{-(p-2)} = g^{a^p}$. Hence $a^p \equiv 1 \pmod q$.

For $p = 2$, $a^2 \equiv 1 \pmod q$ has two solutions $a = 1$, $a = -1$ which give $\mathbb{Z}/pq\mathbb{Z}$ and D_q.

Now assume p arbitrary, $q \equiv 1 \pmod p$. We know $hgh^{-1} = g^a$ $a \pmod q$
$g = h^p g h^{-p} = g^{a^p} \Rightarrow a^p \equiv 1 \pmod q$. If $a \equiv 1 \pmod q$ then G is abelian.
We can solve this for $a \not\equiv 1 \pmod q$ as well. Why? $(\mathbb{Z}/q\mathbb{Z})^\times$ has order $q - 1 \equiv 0 \pmod p$
So by the Sylow theorem $\exists$ an element a of order p. This a gives a nonabelian group G.

ex $pq = 3 \cdot 7 = 21$ $\langle e, g, g^2, g^3, g^4, g^5, g^6 \rangle = H_7$, $\langle e, h, h^2 \rangle = H_3$ $hgh^{-1} = g^2$

Burnside, Frobenius Any group G of order $p^a q^b$ ($\neq p$) has a non-trivial normal subgroup.

If G is simple and non-abelian then it has even order $> H_2$ a Sylow-2 subgroup.
First non-abelian group w/out any non-trivial normal subgroups (i.e. simple) is
A_5 of order $\frac{120}{2} = 60 = 2^2 \cdot 3 \cdot 5 \leftarrow$ 3 primes.

$\# G = 12 = 2^2 \cdot 3$ Will find five different groups.
$H_2 \subset G$ of order 4. There are 1 or 3 of them
$H_3 \subset G$ of order 3. There are 1 or 4 of them.

At least one of these is normal. If H_3 is not $\exists$ 8 elements of order 3 $\Rightarrow$
remaining four elements are $= H_2 \triangleleft G$.

If both are normal $H_3 \cong \mathbb{Z}/3\mathbb{Z}$, $H_2 \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} \longrightarrow G \cong \mathbb{Z}/12\mathbb{Z} \text{ cyclic} \\ \mathbb{Z}/2 + \mathbb{Z}/2 \longrightarrow G \cong \mathbb{Z}/6 \times \mathbb{Z}/2 \text{ abelian} \end{cases}$

If H_3 is not normal then $\exists$ 4 Sylow-3 subgroups.
Action of G on $S = \{\text{Sylow-3's}\}$ by conjugation, which gives a homomorphism $G \hookrightarrow S_4$
Action is transitive so stabalizer of each Sylow-3 has order $3 \Rightarrow$ each group is it's own stabalizer. Thus only e acts trivially the map is injective G contains 8 elements of order 3 which generate the group and their image in S_4 has order 3 so is even $\Rightarrow G \cong A_4$.
If H_2 is not normal but H_3 is then $\exists$ 3 Sylow-2 subgroups.
If $H_2 \cong \mathbb{Z}/2 + \mathbb{Z}/2$ can see that $G \cong D_6$ (see Artin)
If $H \cong \mathbb{Z}/4\mathbb{Z}$ get something else