CONCLUSION: At least one G-orbit $\mathcal{O}_{U_0}$ must have p^e dividing $|G_{U_0}|$.

On the other hand, one always has $|G_{U_0}|$ dividing $|U_0| = p^e$ because G_{U_0} acts on $U_0 = \{u_1, u_2, \ldots, u_{p^e}\}$ via left-translation and so G_{U_0} decomposes U_0 into G_{U_0}-orbits which are cosets $G_{U_0} \cdot u_i$ having the same size $|G_{U_0} \cdot u_i| = |G_{U_0}|$.

Hence p^e divides $|G_{U_0}|$ which divides $|U_0| = p^e$, so $|G_{U_0}| = p^e$ i.e. G_{U_0} is a Sylow p-subgroup. ∎

11/5/2018 >

proof of Sylow's 2nd Thm: Given any p-subgroup $H < G$, if we can show $H < gPg^{-1}$ for some particular Sylow p-subgroup $P < G$ then this will show both parts (take $H = P'$ any other Sylow-p-subgroup to conclude $\cancel{P}P' = gPg^{-1}$).

Consider H acting on $S := \{\text{left cosets } gP : g \in G\} = G/P$ via left-translation, i.e. $h * gP := hgP$

As usual, $|S| = \sum_{\substack{H\text{-orbits } \mathcal{O}_s \\ \text{in } S}} |\mathcal{O}_s| = \sum_{\substack{H\text{-orbits } \mathcal{O}_s \\ \text{in } S}} \underbrace{\frac{|H|}{|H_s|}}$

$\equiv 0 \bmod p$ unless $H_s = H$ (since H is a p-group)

$|S| = |G/P| = \frac{p^e m}{p^e} = m \not\equiv 0 \bmod p$

Hence $\exists$ some $\cancel{\text{coset}}$ $s \in S = G/P$ with $H_s = H$, i.e. $\exists$ some coset gP with $hgP = gP \ \forall h \in H$

$g^{-1}hgP = P$

$g^{-1}hg \in P$

$h \in gPg^{-1}$, i.e. $H < gPg^{-1}$ ∎

proof of Sylow's 3^{rd} theorem: Let $S := \{\underline{all}$ Sylow p-subgroups $P < G\}$
and $s_p := |S|$. Want to show (a) s_p divides m if $|G| = p^e m$
(b) $s_p \equiv 1 \mod p$.

For (a), consider the action of G on S via conjugation:

$$g * P := gPg^{-1} \leftarrow \text{another Sylow } p\text{-subgroup}$$

Sylow's 2^{nd} Thm $\Rightarrow$ this action of G is transitive, i.e. if P_0 is one particular Sylow p-subgroup then

$$S = \mathcal{O}_{P_0}$$

$$\Rightarrow \underbrace{|S|}_{= s_p} = \frac{|G|}{|G_{P_0}|} = \frac{p^e m}{|G_{P_0}|} = \frac{p^e m}{|N_G(P_0)|}$$

where $G_{P_0} = \{g \in G : gP_0g^{-1} = P_0\}$ =: the normalizer subgroup $N_G(P_0)$ of P_0 in G

However $P_0 < N_G(P_0)$ since $g_0 P_0 g_0^{-1} \subset P$ $\forall g_0 \in P_0$,

so $p^e = |P_0|$ divides $|N_G(P_0)|$ $\Rightarrow$ $s_p = \frac{p^e m}{|N_G(P_0)|}$ divides m.

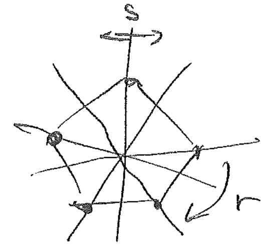
For (b), consider the same action by conjugation on S,
but restricted to P_0, i.e. $g_0 * P := g_0 P g_0^{-1}$ $\forall g_0 \in P_0$

Then $s_p = |S| = \{\text{all Sylow } p\text{-subgroups } P\} = \sum_{P_0\text{-orbits } \mathcal{O}_P} |\mathcal{O}_P|$

$$= \underset{\substack{\mathcal{O}_{P_0} = \{P_0\} \text{ is} \\ \text{a singleton orbit}}}{1} + \sum_{\substack{P_0\text{-orbits} \\ \mathcal{O}_P \neq \{P_0\}}} \underbrace{\frac{|P_0|}{|(P_0)_P|}}_{\text{a power of } p}$$

Then $s_p \equiv 1$ since There are no other singleton orbits $\mathcal{O}_P$, else $P_0 < N_G(P)$ i.e. $g_0 P g_0^{-1} \subset P$ $\forall g_0 \in P_0$
and hence P_0, P are both Sylow p-subgroups of $N_G(P)$
so conjugate within $N_G(P)$. But $P \triangleleft N_G(P)$,
so $P_0 = P$ ∎

§7.9, 7.10 Free groups & generators & relations



We want to make more sense of statements like

"D_n is generated by s, r with $s^2 = 1 = r^n$, $srs = r^{-1}$
and you don't need any further relations"

Start by making sense of a group generated by some set $S = \{a, b, c, \ldots\}$ (called an alphabet) with no relations at all, except those imposed by rules of groups, called the free group $F(S)$ on alphabet S.

EXAMPLES:

① If $S = \{a\}$ then $\overset{F(\{a\})}{\overset{\shortparallel}{F(S)}} = \{\ldots, \overset{a^{-1}a^{-1}}{\overset{\shortparallel}{a^{-2}}}, a^{-1}, 1, a^1, \overset{a \cdot a}{a^2 =}, \ldots\} \cong \mathbb{Z}^+$ (cyclic)

with $a^k \cdot a^\ell = a^{k+\ell}$ e.g. $a^5 \cdot a^{-2} = a^3$

② If $S = \{a, b\}$, $\underset{F(\{a,b\})}{\underset{\shortparallel}{F(S)}}$ ought to contain $1, a, a^2, a^{-3}, \ldots$

$b, b^2, b^{-3}, \ldots$

$ab, ab^2, a^{10}b^{-5}, \ldots$

$ba^7b^{-2}a^{-3}b^{-1}a^2$, etc.

with $b^6a^{-2} \cdot a^{10}b^{-1}a = b^6a^8b^{-1}a$, and so on.

But does this really define a group? Let's be careful, since two different words $w = w_1 w_2 \cdots w_\ell$ with letters in a, a^{-1}, b, b^{-1}, can represent the same element, e.g. $aa^{-1}ab = ab$

DEF'N: Given alphabet $S = \{a, b, c, \ldots\}$, say word $w = w_1 w_2 \cdots w_\ell$ in $S \sqcup S^{-1} = \{a, a^{-1}, b, b^{-1}, c, c^{-1}, \ldots\}$ is reduced if there are no adjacent $(w_i, w_{i+1}) = (x, x^{-1})$ or (x^{-1}, x). Say $w \to w'$ if $w = Axx^{-1}B$ or $Ax^{-1}xB$, $w' = AB$ for some words A, B

and say w' is a reduction of w if $\exists\ w = w_0 \to w_1 \to \cdots \to w_t = w'$.

(106)

LEMMA: Every word w in $S \sqcup S^{-1}$ has a unique reduction w_{red} which is reduced.
(PROP 7.9.2)

27/7/2018

proof: Induct on l in $w = (x_1, x_2, \ldots, x_l)$ for both the existence & uniqueness.
(Existence is clear by induction.)
In the base case where w is already reduced, $w_{red} = w$ is unique!

In the inductive step, assume w has two different reductions w_r, w'_s, both reduced:

$$\begin{tikzcd}
 & w_1 \arrow[r] & w_2 \arrow[r] & \cdots \arrow[r] & w_r \arrow[d, phantom, "\neq"] \\
w \arrow[ur] \arrow[dr] & & & & {} \\
 & w'_1 \arrow[r] & w'_2 \arrow[r] & \cdots \arrow[r] & w'_s
\end{tikzcd}$$

CASE 1: $w_1 = w'_1$ (which could happen either as $w = Axx^{-1}B \to w_1 = AB \to \ldots$, $\to w'_1 = AB \to \ldots$

or as $w = Axx^{-1}xB \to w_1 = AxB \to \ldots$, $\to AxB \to \ldots = w'_1$)

But then w_1 is shorter than w and has two different reduced reductions; contradiction to inductive hypothesis.

CASE 2: $w_1 \neq w'_1$

So one must have this picture:

$$\begin{tikzcd}
 & w_1 = ABy^{-1}yC \arrow[r] \arrow[dr, dotted] & w_2 \arrow[r] & \cdots \arrow[r] & w_r \\
w = Axx^{-1}By^{-1}yC \arrow[ur] \arrow[dr] & & ABC \arrow[r, dotted] & \cdots \arrow[r] & w''_t \\
 & w'_1 = Axx^{-1}BC \arrow[r] \arrow[ur, dotted] & w'_2 \arrow[r] & \cdots \arrow[r] & w'_s
\end{tikzcd}$$

all 3 reduced, and possibly $w''_t = w_r$ or $w''_t = w'_s$

But since either $w_r \neq w''_t$, or $w'_s \neq w''_t$, either w_1 or w'_1 has different reductions that are both reduced; contradiction again ∎

DEF'N: The free group $F(S)$ on a set S is the collection of all equivalence classes of words in $S \sqcup S^{-1}$ for the equiv. relation $w \sim w'$ if $w_{red} = w'_{red}$ with multiplication

$$F(S) \times F(S) \to F(S)$$
$$([u], [v]) \mapsto [uv]$$

$u = u_1 \cdots u_l$, $v = v_1 \cdots v_m$, $uv = u_1 \cdots u_l v_1 \cdots v_m$ called concatenation