Proof of Cauchy's Theorem

prime

Theorem: Let G be a finite group of order n. If $p|n$, then G has a subgroup of order p.

Remark: We have already proved this for *abelian* groups.

Proof: We will use induction on n and the class equation which says that

$$\underline{|G|} = \underline{|Z(G)|} + \sum_{i=1}^{k} [\underline{G : C(x_i)}]$$

where $x_1, \ldots, x_k$ are representatives for the distinct conjugacy classes of size greater than 1.

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C(x_i)]$$

$$\underbrace{|G|}_{p \mid \text{this}} = \underbrace{|C(x_i)|}\underbrace{[G : C(x_i)]}_{p \nmid \text{this}}$$

If the index $[G : C(x_i)]$ is not divisible by p, then the order of the group $C(x_i)$ must be divisible by p. Since $C(x_i)$ is smaller, by induction it contains a subgroup of order p which in turn is a subgroup of G of order p.

if $p \mid C(x_i)$, since $|C(x_i)| < |G|$

By induction $H \subseteq C(x_i)$ of order p.

$H \subseteq C(x_i) \subseteq G$

Therefore all of the indices are divisible by p. However, in that case $|Z(G)|$ must be divisible by p as well.

$$\underbrace{|G|}_{\text{divisible by } p} = |Z(G)| + \sum_{i=1}^{k} \underbrace{[G : C(x_i)]}_{\text{all divisible by } p}$$

this must be divisible by p.

Since $Z(G)$ is abelian and of order divisible by p, it contains a subgroup of order p.

H has p elements $\quad H \subseteq Z(G) \subseteq G$

$\Longrightarrow$ H is a subgp of G with p elements.

p-groups

Corollary: Let p be a prime. The two conditions:

a) • The order of G is a power of p
b) • Every element of G has order that is a power of p

are equivalent.

Groups satisfying (either of) these conditions are called p-groups.

a $\Rightarrow$ b by Lagrange

$x \in G$, order$(x) \mid |G| = p^r \Rightarrow$ order$(x) = p^s$ $0 \le s \le r$

b $\Rightarrow$ a

$|G| \neq p^r \Rightarrow$ ~~b~~ G has an element x
$q \mid |G|$. of order $= q$ q prime $\neq p$.

Quaternion group : 8 elements, not abelian
is a 2-group.

Proof of Sylow's First Theorem

Theorem: Let G be a finite group of order n. If p^r divides n, then G has a subgroup of order p^r.

Proof: As in the proof of Cauchy's theorem consider the class equation

$$|G| = \underline{|Z(G)|} + \sum_{i=1}^{k} \underline{[G : C(x_i)]}.$$

and use induction on n. Assume $r > 1$, otherwise we are done by Cauchy's theorem.

$p^r \,\|\, |G|$ $\quad \underline{r > 1}$.

If any of the $[G : C(x_i)]$ are not divisible by p, then $C(x_i)$ is divisible by p^r and by induction contains a subgroup with p^r elements.

$[G : C(x_i)]$ is not divisible by p^r

$|C(x_i)|$ is divisible by p^r.

$$\underbrace{|G|}_{p^r} = \underbrace{|C(x_i)|}_{p^r}\,\underbrace{[G : C(x_i)]}_{\text{not divisible by } p}$$

$C(x_i)$ has order divisible by p^r

$|C(x_i)| < |G|$ by induction $C(x_i)$ has

a subgp H with p^r elements. $H \subseteq G$ and

so we found a subgp with p^r elts.

If all of the $[G : C(x_i)]$ are divisible by p, so is $|Z(G)|$ so $Z(G)$ has a subgroup H of order p.

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C(x_i)]$$

$p \mid$ ~~this~~ $\quad$ p divides this $\quad$ p divides these

$\exists$ an $H \leq Z(G)$ with $|H| = p$.

This subgroup is necessarily normal since it consists of elements that commute with all of G. $\quad H \subseteq Z(G) \Rightarrow gH = Hg$

$gx = xg$ for all $x \in H$.

The group G/H has order n/p. This is still a multiple of p by the assumption $r > 1$ and so G/H has a subgroup of order p^{r-1}. Let K be this subgroup.

G/H has n/p elts, which is a multiple of p^{r-1}

$|G/H| < |G|$, G/H has a subgroup K with p^{r-1} elts.

The inverse image of K under the canonical homomorphism $G \to G/H$ is a subgroup of G of order p^r.

$G \longrightarrow G/H$

$g \in G \mapsto gH \in G/H$

p to 1

$\{g' \mid g'H = gH\}$ $\quad gH \in G/H$

$\Updownarrow$

$g' \in gH$ which has p elements.

$K \subseteq G/H$

$\tilde{K} = \{g \in G \mid gH \in K\}$

$\tilde{K} \subseteq G$

has p^r elements.

$\tilde{K}$ is the subgroup we are looking for.