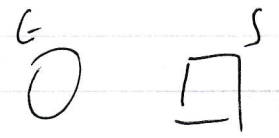
21-373 10/5/2020

Group Action G acting on S 

1) $1_G \cdot x = x \quad \forall x \in S$
2) $\forall g,h \in G, \forall x \in S \quad (gh)\cdot x = g\cdot(h\cdot x)$

Stabilizer of S $\quad G_x = \{g \in G \mid g\cdot x = x\} \quad \forall x \in S$

Theorem: $\forall x \in S$, $G_x \leq G$.

Proof
- Using (1), $1_G \in G_x$.
- Given $g,h \in G_x$, enough to show $(gh)\cdot x = x$ and $g^{-1}\cdot x = x$

$(gh)\cdot x \overset{(2)}{=} g\cdot(h\cdot x) = g\cdot x = x \Rightarrow gh \in G_x$
(h is stabilizer; $g \in G_x$)

"
$g\cdot x = x \Rightarrow g^{-1}\cdot(g\cdot x) = g^{-1}(x)$
$1\cdot x = g^{-1}\cdot x$.
$x = g^{-1}x \Rightarrow g^{-1} \in G_x$.

Orbit$(x) := \{g\cdot x \mid g \in G\}$

Fundamental Theorem of Group Actions Suppose G acts on S. Then for every $x \in S$,
$|\text{orbit}(x)| = [G : G_x]$ index of stabilizer

Proof. Find bijection from orbit(x) onto the left coset $\{hG_x \mid h \in G\}$.
For $h \in G$, let $\varphi(hG_x) := h\cdot x$
Given $h_1, h_2 \in G$. let $h_1G_x = h_2G_x \Leftrightarrow h_2^{-1}\cdot h_1 \in G_x \overset{\text{def of } G_x}{\Leftrightarrow} h_1\cdot x = h_2\cdot x \Leftrightarrow \varphi(h_1G_x) = \varphi(h_2G_x)$
$[(h_2^{-1}h_1)\cdot x = x]$, Hence φ is both well-defined and injective
$\Leftrightarrow h_2\cdot[(h_2^{-1}h_1)\cdot x] = h_2\cdot x$
$\Leftrightarrow h_1\cdot x = h_2\cdot x$

Surjectivity: Given $h \in G$, take $A = h \in X$. $\varphi(A) = h \cdot x$.

Example (1) let $(F, +, \cdot, 0, 1)$ be a field, $S = F$.

$G = (F^\times, \cdot, 1)$, G acts on S by $g \cdot x = g$ times x

(2) let H be a group. $G = Inn(H) = \{f_h \mid h \in H\}$ where $f_h(x) = hxh^{-1}$.
his fixed.

Claim: G acts on H $\quad g \cdot x = f_h(x)$

where $g \in G$ (let $h \in H$ s.t. $y = f_h$)

given $h \in H, x \in H$
$f_h \cdot x := hxh^{-1}$.

$G = Inn(H) \leq Per(H)$
$= \{f_h \mid h \in H\}$

$g \cdot x = h \cdot y$
$\Rightarrow x = g^{-1} h y$

$\rightarrow 1 \cdot x = 1 \times 1^{-1} = x$

$\rightarrow (ab) \cdot x = (ab) x (ab)^{-1} = a(bxb^{-1})a^{-1} = f_a(f_b(x))$
$= a \cdot (b \cdot x)$
(def of action)

$\exists g$ s.t. $gx = a$
$\Rightarrow \exists h$ s.t. $hy = a$

Take $b \in$ orbit x.
$b = hx$
(Recall)

exist h and k
s.t. $b = kx$
$= k g^{-1} h y$
$= hy$

Let E be an equivalence relation on a finite set S. Then $\exists S^* \subseteq S$ s.t.
"representative" $S = \bigcup_{x \in S^*} [x]$ and $x \neq y \in S^* \Rightarrow [x] \cap [y] = \emptyset$.

$orbit(x) = \{g \cdot x \mid g \in G\}_{x \in S}$

Lemma. Suppose G acts on S, then $\forall x, y \in S$ either

1) $orbit(x) = orbit(y)$ or 2) $orbit(x) \cap orbit(y) = \emptyset$

$\neg$ [$a \in orbit(x)$ and $a \in orbit(y)$]
$\Rightarrow$ [$orbit(x) \subseteq orbit(y)$]

Moreover, let $x \sim y \Leftrightarrow x \in orbit(y)$ is an eq relation on S and $orbit(x) = [x]_\sim$.

21-373 $x \sim y \in$ we can prove $x \in \text{orbit}(y)$ by symmetry, reflexivity, and transitivity 10/7/2020

Corollary. If $|G| = p^n$, p is prime, then $|Z_1(G)| \neq 1$

Recall: G acts on itself by inner automorphisms.

For $x \in G, g \in G$, $g \cdot x = gxg^{-1}$

↑ let this be a group action [verify (1) $1 \cdot x = x$ (2) $g \cdot (h \cdot x) = (g \cdot h) \cdot x$

Proof.

Note. $x \in Z(G) \iff \text{orbit}(x) = \{x\}$ [i.e. $|\text{orbit}(x)| = 1$]

under.

$(\forall g \in G)\ gx = xg \iff gxg^{-1} = x \iff \{x\} = \text{orbit}(x) = \{g \cdot x \mid g \in G\}$ ← group action

$= \{gxg^{-1} \mid g \in G\}$

$G = Z(G) \overset{\text{disjoint}}{\cup} \{\text{orbit}(x) \mid x \in G \text{ s.t. } |\text{orbit}(x)| \geq 2\}$

Pick $S^* \subseteq G$ s.t. $x \neq y \in S^* \iff \text{orbit}(x) \cap \text{orbit}(y) = \emptyset$ i.e. "representatives"

$$G = Z(G) \cup \bigcup_{x \in S^*} \text{orbit}(x)$$

$$|G| = |Z(G)| + \sum_{x \in S^*} |\text{orbit}(x)| \quad \text{"fundamental theorem"}$$

$$|Z(G)| = |G| - \sum_{x \in S^*} |\text{orbit}(x)| = p^n - \sum_{x \in S^*} [G : G_x]$$

Since $x \in S^* \Rightarrow |\text{orbit}(x)| \geq 2 \Rightarrow [G : G_x] \geq 2$. By Lagrange, since p is prime and $[G : G_x] \mid p^n$, there is another prime $k_x \geq 1$ s.t. $[G : G_x] = p^{k_x}$

$= p^n - \sum_{x \in S^*} p^{k_x}$

$= p^n - p \sum p^{k_x - 1}$

$= p[p^{n-1} + \Sigma]$

$= p \cdot m$

So $|Z(G)| = p \cdot m, m \geq 1$. $|Z(G)| \geq p\ (> 1)$.

Midterm 1 Review

- Group Actions
- $H \leq G$ (Subgroup characterizations)

  $Z(G) \leq G \ldots$
- Left cosets, Right cosets $Hx = Hy \iff xy^{-1} \in H$ $x \in Hx$

  $xH = yH \iff x^{-1}y \in H$
- Lagrange $|G| = p$ prime $\Rightarrow G$ cyclic.
- Homomorphisms $\varphi : G \to H$ $\varphi(x^{-1}) = \varphi(x)^{-1} \cap \varphi(1_G) = 1_H$

  $\ker(\varphi)$: $\{ g \in G \mid \varphi(g) = 1_H \}$
- Example. $\det : GL(n, F) \to F^*$ homomorphism

  $\ker(\cdot) = SL(n, F)$ $\setminus \det() = 1$.
- Inner Automorphism

21-373 10/12/2020

MT1 Review

Homomorphisms. ($\varphi: G \to H$ Homo)

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$$

Lemma φ is injective $\Leftrightarrow \ker\varphi = \{1_G\}$. [in MT1]

(Parallel in Lin. Alg: $T: V \to W$ linear transformation is injective $\Leftrightarrow$ Null$(T) = \{0\}$)

abelian group wrt addition

Proof ($\Rightarrow$) $x \in \ker\varphi \Rightarrow \varphi(x) = 1 \Rightarrow x = 1_G$.

($\Leftarrow$) $\varphi(x) = \varphi(y) \Rightarrow \varphi(x)\cdot\varphi(y)^{-1} = 1_H$

$\Rightarrow \varphi(x)\varphi(y^{-1}) = 1_H$

$\Rightarrow \varphi(xy^{-1}) = 1_H$

$xy^{-1} \in \ker(\varphi)$.

Theorem. $|G| = p^n$, p is prime $\Rightarrow Z(G) \neq \{1\}$.

Lemma. Suppose G acts on a fixed set S, not necessarily a group

Let $S_0 = \{x \in S \mid (\forall g \in G)\, g\cdot x = x\}$

Lemma! **If $|G| = p^n$ where p is prime, then $|S| \equiv |S_0| \bmod p$.**

Recall: ① If G acts on S, orbit(x) is the equivalent class of x with respect to

$x \sim y \overset{\text{def}}{\Leftrightarrow} \exists g \in G,\ y = g\cdot x$

② $\exists S^* \subseteq S$, $S = \bigcup_{x \in S^*}$ orbit(x), $x \neq y \Rightarrow$ orbit$(x) \cap$ orbit$(y) = \emptyset$

Proof of lemma. $x \in S_0 \Leftrightarrow |\text{orbit}(x)| = 1$

→ $x \in S_0 \Leftrightarrow |\text{orbit}(x)| = 1$ (repeated)

→ Take $S^* \subseteq S$ s.t. $x \neq y \Rightarrow \text{orbit}(x) \cap \text{orbit}(y) = \emptyset$ and (representative)

$$x \in S^* \Rightarrow |\text{orbit}(x)| \geq 2.$$

$$S = S_0 \cup \bigcup_{x \in S^*} \text{orbit}(x)$$

$$|S| = |S_0| + \sum_{x \in S^*} |\text{orbit}(x)|$$

$$|S| - |S_0| = \sum_{x \in S^*} |\text{orbit}(x)| = \sum_{x \in S^*} [G : G_x]$$

$|\text{orbit}(x)| = [G : G_x]$

$$= \sum_{x \in S^*} \frac{|G|}{|G_x|} \quad \text{(by Lagrange)}$$

$g \cdot x \to gG_x$

$|G| = |G_x|[G : G_x]$

$p \mid |G|$, $p \mid |G_x| \Rightarrow p \mid [G : G_x]$

$$= \sum_{x \in S^*} p^{k_x}, \text{ where } k_x \geq 1 \text{ since } |G : G_x| \geq 2$$

$$= p\left(\sum_{x \in S^*} p^{k_x - 1}\right)$$

$$p \mid |S| - |S_0| \Rightarrow |S| \equiv S_0 \mod p.$$

Now let $S = G$, consider the action of G on S by $g \cdot x = gxg^{-1}$ $\forall g \in G$

$$S_0 = \{x \in G \mid (\forall g \in G)\, g \cdot x = x\} = \{x \in G \mid (\forall g \in G)\, gxg^{-1} = x\}$$

$$= \{x \in G \mid (\forall g \in G)\, gx = xg\}$$

$$= Z(G)$$

By the lemma, $|G| \equiv |Z(G)| \mod p$

As $|G| = p^n \equiv 0 \mod p \Rightarrow |Z(G)| \equiv 0 \mod p$.

Since $1_G \in Z(G)$, $|Z(G)| \geq 1 \Rightarrow |Z(G)| \geq p$.

21-373

(Cauchy) Suppose G is a finite group.
If p is prime, s.t. $p \mid |G|$, then $\exists H \leq G$, $|H| = p$.

(Sylow) If G is finite, p prime, s.t. $p^k \mid |G|$, then $\exists H_k \leq G$ s.th., $|H_k| = p^k$.

Proof. Let $S = \{(a_0, \ldots, a_{p-1}) \mid a_i \in G, \prod_{i=0}^{p-1} a_i = 1_G\}$

Note $S \neq \emptyset$ since $(1, \ldots, 1) \in S$

Take $H = \mathbb{Z}/p\mathbb{Z}$ action of H on S by ~~cyclic~~ counter-clockwise rotation

$\bar{0} \cdot (a_0, \ldots a_{p-1}) = (a_0, a_1 \ldots a_{p-1})$

$\bar{1} \cdot (a_0, \ldots a_{p-1}) = (a_1 \ldots a_{p-1} a_0)$

$\bar{2} \cdot (\quad) = (a_2 \ldots a_{p-1} a_0 a_1)$

$\bar{p-1} \cdot (a_0 \ldots a_{p-1}) = (a_{p-1} a_0 \ldots a_{p-2})$ "equivalence class has only 1 element"

$S_0 = \{(a_0, \ldots, a_{p-1}) \mid \prod a_i = 1, \forall (h \in H)\ h \cdot (a_0, \ldots, a_{p-1}) = (a_0, \ldots, a_{p-1})\}$

$(x_0 \ldots x_{p-1}) \in S_0 \Rightarrow a_0 = x_1$ act: rotate by $\bar{1}$ $(x_1, x_2, \ldots, x_{p-1}, x_0)$

$\Rightarrow a_0 = x_2$ $\bar{2}$ $(x_2, x_3, \ldots, x_{p-1}, x_0, x_1)$

Suppose $x_1 \neq x_2$

$\Rightarrow x_0 = x_1 = \ldots = x_{p-1} \in G$

Better Proof in DF Pg 96

Then we conclude $S_0 = \{(a_1, \ldots a_p) \mid \prod a_i = a^p = 1\}$ so S_0 is not empty.

pick first $p-1$ elements then select correct last element

By the lemma, $|S| \equiv |S_0| \bmod p$. Since $|S| = |G|^{p-1}$

So $|G|^{p-1} \equiv |S_0| \bmod p$. But $p \mid |G|$ so $|G|^{p-1} \equiv 0 \bmod p$

$|S_0| \equiv 0 \bmod p$, $|S_0| \geq p$. exists $a \neq 1$, $H = \{1, a \ldots a^{p-1}\} \leq G$. ∎

Sylow Theorem Let G be a finite group, p a prime number s.t. $p \mid |G|$.

Let n and m be integers s.t. $|G| = p^n \cdot m$ where $(p, m) = 1$.

Then $\exists P \leq G$ s.t. $|P| = p^n$.

Question $\binom{768}{256}$ even/odd? ($768 = 3 \times 2^8$)

Combinatorial 'lemma' Suppose p is prime, n, m natural numbers, s.t. $(p, m) = 1$.

Then $\binom{mp^n}{p^n} \not\equiv 0 \bmod p$

$(\equiv m \bmod p)$

Proof of Sylow using lemma.

Consider $S := \{X \subseteq G : |X| = p^n\}$ will one of the sets is a subgroup

For $g \in G$, $X \in S$, # let $g \cdot X = \{gx \mid x \in X\}$ X is a set but not necessarily a subgroup. pseudo 'left coset'

Claim: This is an action of G on S.

Proof. $1 \cdot X = X$, $g, h \in G \Rightarrow g \cdot (h \cdot X) = (gh) \cdot X$

There is $A \subseteq S$ s.t. $S = \bigcup_{X \in A} \text{orbit}(X)$ (representatives) and $X \neq Y \in A \Rightarrow \text{orbit}(X) \cap \text{orbit}(Y) = \emptyset$

$$|S| = \sum_{X \in A} |\text{orbit}(X)| = \sum_{X \in A} [G : G_X]$$

$|S| = \binom{|G|}{p^n} = \binom{mp^n}{p^n}$. By the Combinatorial lemma,

$p \nmid \binom{mp^n}{p^n} (= |S|)$

From $p \nmid |S|$ and $|S| = \sum_{X \in A} |\text{orbit}(X)| = \sum_{X \in A} [G : G_X]$

$\exists X \in A$, $p \nmid [G : G_X]$. This G_X is what we want!

By Lagrange, $|G_X| = \frac{|G|}{[G : G_X]} = p^n \cdot m'$ for some $n, m' \leq m$.

This means $|G_X| \geq |X|$.

pick $a_0 \in X$ Define $f : G_X \to X$ by $f(g) = g \cdot a_0$

Since $g \in G_X$, $g a_0 \in X$

Claim: f is injective.

Proof: $f(g_1) = f(g_2) \Rightarrow g_1 a_0 = g_2 a_0 \Rightarrow g_1 = g_2$

Hence $|G_X| \leq |X| \ (= p^n)$

Conclusion: $|G_X| = |X| = p^n$, and $\#G_X \leq G$.

4.1 Q1 (not used in hw)

1. $b = g \cdot a$

($\Rightarrow$) $x \in \mathrm{Stab}_b \Rightarrow x \in g\,\mathrm{Stab}_a g^{-1}$.

$x \cdot b = b \Rightarrow x \cdot (g \cdot a) = g \cdot a$

$(g \cdot a) \in A$

($\Leftarrow$)

$x \in g\,\mathrm{Stab}_a g^{-1}$. $x = gyg^{-1}$, $y \cdot a = a$

$g^{-1}x = yg^{-1}$, $y \cdot g^{-1} \cdot a = a$

$y \cdot g^{-1} \cdot b = a$.

$x \cdot b = gyg^{-1} \cdot b = gyg^{-1}(g \cdot a) = gya = g \cdot a = b$.

$\in$ is transitive $\ker(\in)$

$g \cdot a \cdot g^{-1} = a$.

$g \cdot b$

$k \cdot a = a \ \forall a \in A$

$x = gyg^{-1}$, $y \cdot a = a$.

$= y$, $\boxed{x = gyg^{-1}}$

$g^{-1} \cdot x \cdot g \cdot a = a$.

$(x \cdot g) \cdot a = g \cdot a$

g^{-1}

For any $a, b \in A$, $\exists g$ s.t. $a = g \cdot b$

$k \in g\,\mathrm{Stab}_a g^{-1} = \mathrm{Stab}_b$

k must stabilize b, $b = g \cdot a$.

$k \in \ker(G) \Leftrightarrow k \cdot a' = a' \ \forall a' \in A$

$\Leftrightarrow k \cdot g \cdot b^a = g \cdot b^a \ \forall g \in \in$ (a fixed)

$\Leftrightarrow k$

$k \in g\,\mathrm{Stab}_{a'} \ \forall a' \in A$

$\Leftrightarrow k \in g\,\mathrm{Stab}_a g^{-1} \ \forall g \in \in$

$|S| \cdot |\mathrm{Stab}| \ | \ \in : C(\in)| = n$

$C(\in) \subseteq C_{\in}(S)$

n

$\frac{2\pi i k}{p^k} + \frac{2\pi i \ell}{p^\ell}$

$g \cdot a = gag^{-1}$

$gNg^{-1} \in N$, $N \leq \in$

$N = G$,

$n \cdot a = gx$

A B

$\{\mathrm{Stab}_a \mid a \in A\} = \{g\,\mathrm{Stab}_b g^{-1} \mid g \in \in\}$

$A \subseteq B$: follows from transitivity and first part

$g \in A \Rightarrow s \in B$

$g_1 C \quad g_2 C \quad g_3 C \quad g_4 C \quad g_5 C \Rightarrow gC \subseteq G/N$

$g_1, g_2 \in X \quad H \leq K \leq G$

$n = ? \cdot 1^+$

$e^{\frac{2\pi i \cdot t}{p^k}}, t \in [0, p^k)$

$x \in g_1 C$

$g_1 \; g x g^{-1} g_1 C$

$y^T \cdot \hat{y} - \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} - \begin{bmatrix} \\ \\ \\ \\ \\ \end{bmatrix}$

$z^{p^3} = 1 \Rightarrow z^{p^2} = 1?$

(a) $\Rightarrow H_k \subseteq H_m \quad z \in H_k \Rightarrow z \in H_m$

Knows $z^{(p^k)} = 1 \Rightarrow z^{(p^m)} = 1.$

$z^{p^m - p^k} = 1.$

let $z = e^{\frac{2\pi i}{p^3}}$. $z^{p^2} = e^{\frac{2\pi i}{p}}$ $t^{p^k} \cdot p^{m-k} = \boxed{(t^{p^k})^{p^{m-k}}} \neq 1.$

$e^{2\pi i (p^{m-k})} = 1.$

$\Leftarrow \quad k \leq m.$

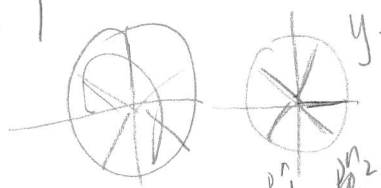
$(a^b)^c = a^{bc}$

wts $z^{(p^k)} = 1 \Rightarrow z^{(p^m)} = 1.$

$z^{(p^k) \cdot p^{m-k}} = \left[z^{(p^k)}\right]^{p^{m-k}} = 1^{p^{m-k}} = 1.$

(b) $e^{\frac{2\pi i}{p^k}}$ is generator. $(z^1)^{p^k} = 1.$

(c)



$p_1^{n_1} p_2^{n_2}$

$z_1^{p^{n_1}} \cdot z_2^{p^{n_2}} = 1.$

$z_1^{p^{n_1}} = 1 \qquad (n_1, n_2) = 1.$

$z_1^{p^{n_1}} \cdot z_2^{-p^{n_2}} = 1$

(d) $(t^a)^b = t^{a \cdot b}$

$H \geq H_k \checkmark$

$H \subseteq H_k$

$n_1 \nmid n_2?$

$y \cdot \hat{y} - \hat{y} + \hat{y} - y \cdot \hat{y}$

$\ell(\hat{y}, y) = -y_1 \log(\hat{y}_1) - y_2 \log(\hat{y}_2) - y_3 \log(\hat{y}_3)$

$d\hat{y}\,\ell \quad \frac{d\ell}{\hat{y}_1} = -\frac{y_1}{\hat{y}_1}, \quad \frac{d\ell}{\hat{y}_2} = -\frac{y_2}{\hat{y}_2}$

$\frac{d\hat{y}_1}{db_1} = \hat{y}_1(1 - \hat{y}_1) \quad \frac{d\hat{y}_2}{db_1} = \hat{y}_2(-\hat{y}_1)$

$\frac{d\hat{y}_1}{db_2} = \hat{y}_1(-\hat{y}_2) \quad \frac{d\hat{y}_1}{db_2} = \hat{y}_2(1 - \hat{y}_2)$

$\frac{d\hat{y}_1}{db_3} = \hat{y}_1(-\hat{y}_3) \quad \frac{d\hat{y}_2}{db_3} = \hat{y}_2(1 + \hat{y}_3)$

$\frac{d\ell}{db_1} = \frac{d\ell}{d\hat{y}_1} \cdot \frac{d\hat{y}_1}{db_1} + \frac{d\ell}{d\hat{y}_2} \cdot \frac{d\hat{y}_2}{db_1} + \frac{d\ell}{d\hat{y}_3} \cdot \frac{d\hat{y}_3}{db_1}$

$= \frac{-y_1}{\hat{y}_1} \cdot \hat{y}_1(1 - \hat{y}_1)$

$+ \frac{-y_2}{\hat{y}_2}(\hat{y}_2)(-\hat{y}_1)$

$+ (-y_3)(\hat{y}_3)(-\hat{y}_1)$

$\frac{d\ell}{db_1} = y_1 \boxed{\hat{y}_1 - y_1} + y_2 \hat{y}_1 + y_3 \hat{y}_1$

$\frac{d\ell}{db_2} = -y_1 + \hat{y}_1(y_1 + y_2 + y_3)$

21-373 10/19/2020

Proof of Combinatorial Lemma

p prime, m natural number s.t. $(m,p)=1$ $\quad \binom{m\cdot p^n}{p^n} \equiv m \bmod p$.

Proof by Group Actions.

Recall fact. let $S_0 = \{x \in S \mid (\forall g \in G)\, g\cdot x = x\}$

$|S| \equiv |S_0| \bmod p$.

let $\in = \mathbb{Z}/p\mathbb{Z}$.

$B = \{1, \dots, p^n\}$, $A = \in \times B$. $|A| = |\in| \cdot |B| = m \cdot p^n$

$S = \{X \subseteq A : |X| = p^n\}$

Define for $g \in \in$, $X \in S$, $g \cdot X = \{(g+a, b) \mid (a,b) \in X\} \subseteq A$, $|g\cdot X| = p^n$.

$|S| = \binom{mp^n}{p^n}$

What is S_0? Need to show $|S_0| \equiv m \bmod p$.

$G = \mathbb{Z}/p^n\mathbb{Z}$, $B = \{1, \dots m\}$, $A = \in \times B$, $S = \{X \subseteq A : |X| = p^n\}$ $g \in \in$, $X \in S$

$g \cdot X = \{(g+a, b) \mid (a,b) \in X\}$

$|S| = \binom{mp^n}{p^n}$

What is S_0? Since $|\in| = |\{a \mid (a,b) \in X\}|$, get $S_0 = \{\in \times \{1\}, \in \times \{2\}, \dots \in \times \{m\}\}$

$\therefore \binom{mp^n}{p^n} \equiv m \bmod p$.

Normal Subgroups

Let G be a group. $N \leq G$ is called normal provided

$\forall g \in G, \forall n \in N, \; gng^{-1} \in N$. Notation $N \triangleleft G$ (or $N \trianglelefteq G$)

(↑ conjugate of n by g)

Proposition. $Z(G) \triangleleft G$. Given $g \in G, n \in Z(G)$

$$(gn)g^{-1} = ng g^{-1} = n \in Z(G)$$

Recall $\forall g \in G$, $f_g(x) = gxg^{-1}$ is the inner automorphism induced by g.

G acts on itself by $g \cdot x = gxg^{-1} = (f_g(x))$

orbit$(x) = \{gxg^{-1} \mid g \in G\}$ — conjugacy class

Remark. Suppose $N \leq G$.

$$N \trianglelefteq G \iff \forall g \in G, \; f_g : N \to N$$

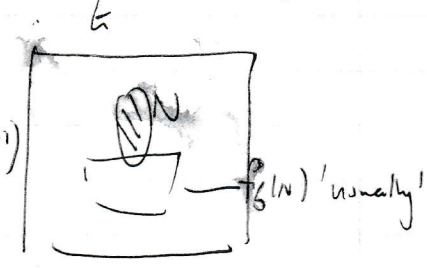
not truly injective but bijective!

Prop. $\varphi : G \to H$ homomorphism $\Rightarrow \ker \varphi \trianglelefteq G$

Proof. Given $g \in G$, $n \in \ker \varphi$, compute

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1})$$
$$= h \cdot \varphi(n) h^{-1}$$
$$= 1_h.$$

$\therefore gng^{-1} \in \ker \varphi$



What stabilizer examples

If s is central $G_s = \{g \in G \mid gsg^{-1} = s\} = N_G(s)$

If s is central, $G_s = C_G(s)$

$\Rightarrow$ Class Equation. $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$

21-373 10/21/2020

TFAE: $N \trianglelefteq G$

(1) $N \trianglelefteq G$ $(\forall g \in G, \forall n \in N, gng^{-1} \in N)$

(2) $(\forall g \in G)\ gN = Ng$

(2) $\Rightarrow$ (1) $\forall g \in G\ gng^{-1} \in N$: Given $n \in N, g \in G$

$gN = Ng \Rightarrow gn \in Ng \Rightarrow \exists n_1 \in N$ s.t. $gn = n_1 g$

$\Rightarrow gng^{-1} = n_1,\ gng^{-1} \in N$

(1) $\Rightarrow$ (2) To show $gN = Ng$ first show $gN \subseteq Ng$.

By $N \trianglelefteq G$, we have for $\forall gn \in gN$ $gng^{-1} \in N$.

$gng^{-1} = n_1$

$gn = n_1 g \in Ng$

Notation. Given $A \subseteq G, g \in G$, $gAg^{-1} := \{gag^{-1} \mid a \in A\}$

$N_G(A) := \{g \in G \mid gAg^{-1} = A\}$ is the normalizer of A.

Remark (1) $N_G(A) \leq G$

(2) $N_G(A) \geq C_G(A)$

(3) $N_G(N) = G$ when $N \subseteq G \Leftrightarrow N \trianglelefteq G$

Def $H \leq G$. Let $G/H := \{aH \mid a \in G\}$ (LC)

Theorem. If $N \trianglelefteq G$ ($\Leftarrow$), then for $x, y \in G$, $(xN) * (yN) := (xy)N$ is well-defined and $(G/N, *)$ is a group. ('Quotient Group')

- Check associativity. $[(xN) * (yN)] * (zN)$
$= (xy)zN = (x(yz))N$
$= (xN) * [(yz)N]$
$= xN * [(yN) * (zN)]$
- Identity $1_G N = N$
$(1_G N) * (xN) = (1_G \cdot x)N = xN$
- Inverse is $y^{-1}N$.

Remark. This is a generalization of $\mathbb{Z}$ mod n.

Given $n, N := n\mathbb{Z}$, $(G/N, *)$ is $\mathbb{Z}/n\mathbb{Z}$. $\{\bar{0}, \bar{1}, \ldots \overline{n-1}\}$

Proof. To show $*$ is a well-defined operation, we need to show if $x, x_1, y, y_1 \in G$ s.t. $xN = x_1N$ and $yN = y_1N$ then $(x_1y_1)N = (xy)N$

$x_1 \in xN \Rightarrow (\exists n_1 \in N)\ x_1 = xn_1$

$y_1 \in yN \Rightarrow \exists m_1 \in N,\ y_1 = ym_1$

$$x_1y_1 = (xn_1)(ym_1) = x(n_1ym_1)$$

added extra term!

$$= x(yay^{-1})(n_1ym_1)$$

$$= (xy)(y^{-1}n_1y)\,m_1$$

since $N \trianglelefteq G$, let this be n_2

$$= (xy)\,n_2 \cdot n_1 = (xy) \cdot n_3, \text{ for some } n_3 \in N.$$

Hence we see that $x_1y_1 \in (xy)N$

$\Rightarrow (x_1y_1)N = (xy)N$

(Since cosets are either equal or disjoint, we have $b \in aN \Rightarrow bN = aN$)

First Isomorphism Theorem

Suppose $\varphi : G \to H$ is a surjective homomorphism, then

$\exists\ \Psi : G/\ker\varphi \cong H$. (understand H by $G/\ker\varphi$)

Proof. let $N := \ker \varphi$. $\psi(aN) := \varphi(a)$.

Show that ψ is homomorphism $\psi((aN)*(bN)) \overset{\text{def}*}{=} \psi(abN)$

$\overset{\text{def}\psi}{=} \varphi(ab)$

$= \varphi(a)\varphi(b)$

$\overset{\text{def}\psi}{=} \psi(aN)\cdot\psi(bN)$

Show that ψ is surjective.

Given $b \in H$, as φ surjective, take $a \in$ s.t. $\varphi(a) = \psi(aN) = b$.

Need to show that ψ is injective.

(c.f. MT1) Need to show $\ker \psi = \{1_{G/N}\}$.

proof $\ker \psi = \{aN \mid \varphi(a) = 1_H\} = \ker \varphi$

$= N$

$= \{1_{G/N}\}$.

21-373 10/26/2020

Recap. $N \trianglelefteq G \Rightarrow (G/N, *)$ is a group, where $G/N := \{aN \mid a \in G\}$ and

$(aN * bN) := (ab)N$.

Important examples: (1) G abelian, $H \leq G \Rightarrow H \trianglelefteq G$

(2) $Z(G) \trianglelefteq G$

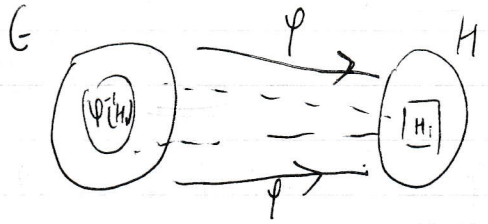
(3) $\varphi: G \to H$ homomorphism, $\ker \varphi \trianglelefteq G$

First Isomorphism. If $\varphi: G \to H$ surjective homomorphism, then $H \cong G/\ker\varphi$ ($N = \ker\varphi$.)

$\Psi(aN) := \varphi(a)$. Check that Ψ hom, surj, Ψ inj ($\ker\Psi = \{N\}$ ← coset)

Remark. $|G/N| = [G:N]$ ← group actions are applied on cosets!

Recall (from HW) $\varphi: G \to H$ homomorphism. Given $H_1 \leq H$, $\varphi^{-1}[H_1] \leq G$. $G_1 \leq G \Rightarrow \varphi[G_1] \leq H$.



Conjugacy class Equation. If G acts on G by inner automorphisms, then

$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : G_x]$ (orbit(x))

≅ conjugate class of x

- If $|G| = p^n$, p is prime, then $|Z(G)| = p^\ell$ for some $\ell \geq 1$.
- (Cauchy) Suppose G is finite, p is prime and $p \mid |G|$, then $\exists\, a \in G - \{e\}$ s.t. $|\langle a \rangle| = p$

(Note prime ⇒ cyclic)

Theorem. If $|G| = p^n$, p is prime, then $\forall k \leq n$, $\exists H_k \leq G$, $|H_k| = p^k$.

Corollary. If $|G| = m \cdot p^n$, p prime, $(m,p) = 1$, $\forall k \leq n$, $\exists H_k \leq G$, $|H_k| = p^k$.

Remark. $H \leq Z(G) \Rightarrow H \trianglelefteq G$.

Given $g \in G$, $h \in H$, we see that $gh = hg$.

$ghg^{-1} = h$. So $H \trianglelefteq G$.

Proof by Induction. $n = 1$ trivial.

Ind: Suppose $|G| = p^{n+1}$. We know $Z(G)$ is non-trivial.

As $|Z(G)| = p^l$ for some $l \geq 1$, apply Cauchy. $\exists a \in Z(G)$ such that $H := \langle a \rangle$ has order p. By the last remark, $H \trianglelefteq G$.

Let $G^* := G/H$. $|G^*| = [G : H] = \frac{|G|}{|H|} = \frac{p^{n+1}}{p} = p^n$.

Trick — 'transform'/'shrink' into quotient space

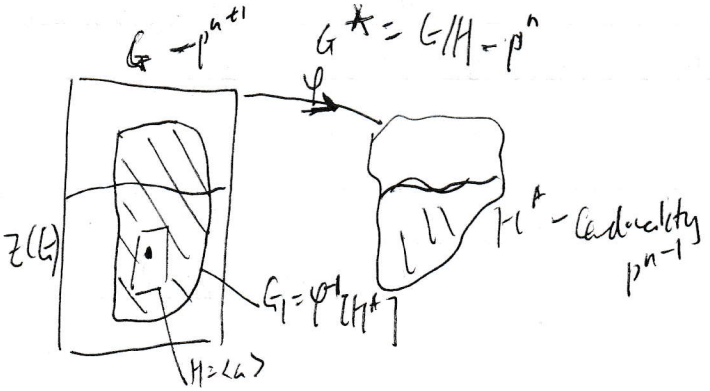
By the inductive hypothesis, $\exists H^* \leq G^*, |H^*| = p^{n-1}$

Let $G_1 = \varphi^{-1}(H^*)$ where $\varphi : G \to G/H$ [the natural homomorphism]

$\varphi(g) = gH \longrightarrow \varphi[G_1] = H^*$, this is surjective! $\varphi(g) = gH$

$|G_1| = [G_1 : H] \cdot |H| = p \cdot p^{n-1} = p^n$.

number of cosets; size of each coset



21-373 10/26/2020

Sylow $\Rightarrow$ Cauchy.

Sylow: $|G| = m \cdot p^n$, p prime, $(m,p)=1$. $\exists H \leq G$, $|H| = p^n$

Cauchy: $p \mid |G|$, p is prime then $\exists H \leq G$, $|H| = p$.

Sylow identifies $|P| = p^n$. Let $b \in P - \{e\}$. By Lagrange, $Q = \langle b \rangle$ satisfies $\exists k \geq 1$ s.t. $|Q| = p^k$.

$Q' = \langle b^{p^{(k-1)}} \rangle$ has $|Q'| = p$.

$a = b^{p^{k-1}}$ $a \neq \{e\}$ since $|Q| = p^k$.

$a^p = (b^{p^{(k-1)}})^p = b^{(p^{(k-1)} \cdot p)} = 1_G$.

21-373 10/28/2020

Isomorphism Theorems

~~$\varphi(h) = (\varphi(h)\ker\varphi)$~~ $\varphi(g\ker\varphi) = \varphi(g)$

First Isomorphism: $\varphi: G \to H$ surjective homomorphism $\Rightarrow H \cong G/\ker\varphi$.

Second " : Given $A, B \leq G$, if $A \leq N_G(B)$ then

$AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A\cap B$.

[Recall that $B \leq G$, $N_G(B) := \{g \in G \mid gBg^{-1} = B\}$ normalizer of B in G. ⇐ $gB = Bg$

Always $B \trianglelefteq N_G(B)$, $A \leq N_G(B) \Rightarrow AB \leq N_G(B)$]

Def $A, B \subseteq G$, $AB = \{ab \mid a \in A, b \in B\}$ So since $B \subseteq AB$, and all elements of AB normalize B, $B \trianglelefteq AB$

Third " : Suppose $H, K \trianglelefteq G$ and $H \leq K$, then

$K/H \trianglelefteq G/H$ and $G/K \cong (G/H)/(K/H)$

'intuition' $(a/c)/(b/c) = \frac{a}{b}$

We attempt to prove the Second

Technical Lemma.

Suppose $H, K \leq G$.

$HK \leq G \Leftrightarrow HK = KH$.

Proof of Lemma. ($\Leftarrow$) $\forall xy \in HK \overset{\text{WTS}}{\Rightarrow} xy^{-1} \in HK$

Given $(h_1k_1), (h_2k_2) \in HK$,

Compute $(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$

$= h_1k_3h_2^{-1}$

$\in KH = HK$

$= h_1h_3k_4 = h_4k_4 \in HK$ ✓

($\Rightarrow$) Let $HK \leq G$. WTS $HK = KH$

$1_G \in H \cap K \Rightarrow K \leq HK$ and $H \leq HK$

$HK \leq G \Rightarrow KH \subseteq HK$ Given $hk \in HK$ w.t.s $hk \in KH$

$(hk)^{-1} = k^{-1}h^{-1} \in HK$, since $k^{-1}h^{-1} \in KH$. $\Rightarrow \exists\, h_1 \in H, k_1 \in K$, $k^{-1}h^{-1} = h_1k_1$ take inv.

'weaker version of normality'.

If $H \trianglelefteq G$ or $K \trianglelefteq G$ then $KH = HK$.

$\rightarrow H \leq N_G(K)$ or $K \leq N_G(H)$ enough.

Corollary. $H \overset{(B)}{\leq} G$, $N \overset{(A)}{\leq} N_G(H)$ then $HN \overset{(B)}{\leq} G$.

Proof Since $\forall h \in H, Nh = hN$, so $HN = NH \overset{\text{Lemma}}{\Rightarrow} HN \leq G$.

a. $AB \leq G$ This is the first part.

$A, B \leq G$, $A \leq N_G(B)$

$A, B \leq G$, $A \leq N_G(B)$. (Easy to see that) $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$:

. Consider $\varphi : A \to AB$ given by $\varphi(a) = \{a\}B$.

b. $A \cap B \trianglelefteq A$

$\ker(\varphi) = \{a \in A \mid aB = 1B\} = A \cap B$

$\{a \in A \mid a \in B\}$

def. right coset $a \cdot 1' \in B$ $\Rightarrow A \cap B \trianglelefteq A$.

$\Updownarrow$

$a \in B$

/ Consider $\Pi : AB \to AB/B$, given by $\Pi(ab) = (ab)B$.

Note that Π is surjective homomorphism (?) $\Pi(z_1 z_2) = z_1 B \cdot z_2 B = \Pi(z_1)\Pi(z_2)$

$\ker(\Pi) = B$. By ~~1st isomorphism applied to~~

~~$AB/B \cong AB/B$.~~ $\psi = \Pi \circ \varphi : A \to AB/B$

$\ker \psi = A \cap B$ $A \xrightarrow{\varphi} AB \xrightarrow{\Pi} AB/B$

By the 1st isomorphism theorem, $\ker(\psi) \to B \to B$

$A/\ker\psi \cong AB/B \cong A/A \cap B$.

($B \trianglelefteq AB$? See previous)

W.T.S $K/K \cap N \cong KN/N$

Find $\chi : K \to KN/N$ surjective homomorphism

Then $NK/N \cong K/\ker\chi$ by 1st isomorphism

Consider $\varphi : K \to KN$ by $\varphi(k) = 1 \cdot k$

$\psi : KN \to KN/N$

$\chi : K \to KN/N$

Show that χ is surjective.

C.

21-373 10/30/2020

3rd Isomorphism Theorem

Suppose $N, K \trianglelefteq G$ and $N \leq K$. Then $K/N \trianglelefteq G/N$, and $\boxed{G/K \cong \frac{G/N}{K/N}}$ ('division')

Proof. Consider $\varphi : G/N \to G/K$ given by $\varphi(gN) = gK$.

(then use 1st Iso to show that $G/K \cong \frac{G/N}{\ker(\varphi)} = \frac{G/N}{K/N}$)

Claim φ is a surjective homomorphism.

Pf. $\varphi((g_1N)\cdot(g_2N)) \overset{N \trianglelefteq G}{=} \varphi((g_1g_2)N) = (g_1g_2)K \overset{K \trianglelefteq G}{=} (g_1K)(g_2K) = \varphi(g_1N)\varphi(g_2N)$

$\ker\varphi = \{ gN \in G/N \mid \varphi(gN) = 1_{G/K} = K \}$

$= \{ gN \mid gK = K \}$

$= \{ gN \mid g \in K \} = K/N.$

Recall that G infinite cyclic then $G \cong (\mathbb{Z}, +)$

(Given $a \in G$, $\langle a \rangle = G$, take $\varphi : \mathbb{Z} \to G$, $\varphi(n) = a^n$.)

Theorem. If G is a cyclic finite group, $|G| = n$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. Pick $a \in G$ s.t. $\langle a \rangle = G$, $G = \{ a^0, a, a^2, \ldots a^{n-1} \}$

Let $\varphi : \mathbb{Z} \to G$, $\varphi(k) = a^k$. φ is homomorphism. $\varphi(k_1+k_2) = (a^{k_1})(a^{k_2}) = \varphi(k_1)\cdot\varphi(k_2)$.
Also, φ is clearly surjective.

By the 1st Isomorphism Theorem, $G \cong \mathbb{Z}/\ker\varphi$, $\ker\varphi = \{ k \in \mathbb{Z} \mid a^k = 1 \} = n\mathbb{Z}$

Book uses $\forall a, b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}, n \in \mathbb{N}$ s.t. $b = qa + r$

$\mathbb{Z}/n\mathbb{Z}$.

Finally groups of order up to some reasonably up to isomorphism.

When $|G| = p$ prime, by Lagrange G is cyclic

$\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$ what we just showed

A group is simple if it does not have a normal subgroup.

$\rightarrow$ cannot take 'quotients'

Corollary: prime numbers

Classification of simple finite groups is extremely difficult.

Gorenstein
Finite Groups

21-373 11/2/2020

Fact: If $|G| = p^n$, p is prime, G acts on S,

def $S_0 = \{x \in S \mid \forall g \in G,\ g \cdot x = x\}$. Then $|S| \equiv |S_0| \bmod p$.

$H \leq G$, $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. ($\Rightarrow H \trianglelefteq N_G(H)$)

Lemma Suppose G is finite, $H \leq G$, p is prime and $|H| = p^n$ for some $n \geq 1$.
Then $[N_G(H) : H] \equiv [G : H] \bmod p$.

Proof Let $S := \{gH \mid g \in G\}$. H acts on S by $\forall h \in H$, $xH \in S$,

$h \cdot (xH) := (hx)H$ Verify that this is a group action.

(1) $1 \cdot (xH) = xH$

(2) $g \cdot (h \cdot (xH)) = (gh) \cdot (xH)$

$\therefore g(hx) = (gh)x$

$S_0 = \{xH : (\forall h \in H)\ (hx)H = xH\}$

$xH \in S_0 \iff (\forall h \in H)\ (hx)H = xH$

($Ha = Hb \iff ba^{-1} \in H$
$aH = bH \in G \iff a^{-1}b \in H$)

coset calculus

$(\forall h \in H)\ x^{-1}(hx) \in H$

$x \in N_G(H)$

$|S_0| = [N_G(H) : H]$, $S_0 \subseteq S$, $|S_0| \equiv |S| \bmod |H|$

$\uparrow [G : H]$

Corollary. Suppose $H \leq G$, $|H| = p^n$, p is prime. $p \mid [G:H]$.
Then $H \lneq N_G(H)$.

Proof. $p \mid [G:H]$, $0 \equiv [G:H] \bmod p$

$\overset{\text{prev lemma}}{\Rightarrow}$ $[N_G(H):H] \equiv 0 \bmod p$ — (1)

But $[N_G(H):H] \geq 1$. — (2)

By (1) and (2), $p \mid [N_G(H):H]$.

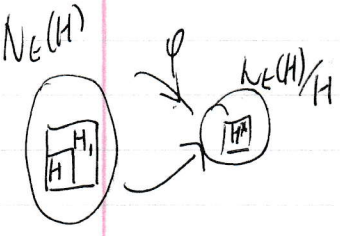
$\Rightarrow H \lneq N_G(H)$.

Sylow's First Theorem Suppose $|G| = p^n \cdot m$, p is prime and $(p,m) = 1$.
Then $\forall k$, $1 \leq k \leq n$, $\exists H_k \leq G$, $|H_k| = p^k$

new ✗ $\forall k$ $1 \leq k < n$, H_k is proper normal subgroup of another subgroup of G.

Proof. By induction on n: $\exists H \leq G$, $|H| = p^k$, $k < n$ (induction hypothesis)
Since $p \mid [G:H]$, $H \trianglelefteq N_G(H)$,

$|N_G(H)/H| = [N_G(H):H] \overset{\text{lemma}}{\equiv} [G:H] \bmod p$



Since $p \mid [G:H]$, $|N_G(H)/H| \equiv 0 \bmod p$

Thus $H \lneq N_G(H)$ & As $p \mid N_G(H)/H$, by Cauchy,

$\exists H^* \leq N_G(H)/H$ s.t. $|H^*| = p$. Let $\varphi: N_G(H) \to N_G(H)/H$ be the natural homomorphism.

L1-373

11/2/2020

Let $H_1 \leq N_G(H)$ s.t. $\varphi(H_1) = H'$, $H_1 = \varphi^{-1}(H')$.

Since H is the identity of $N_G(H)/H$ and $|_{N_G(H)/H} \in H^*$

So $H \leq H_1$ namely $H_1/H = H^*$.

$|H_1| = |H| \cdot |H_1/H| = p^k \cdot p = p^{k+1}$

(Earlier proof of Sylow: $\binom{mp^n}{p^n} \equiv m \bmod p$

Using 1st Fact. $|S| \equiv |S_0| \bmod p$ when acting by $|G| = p^m$.

• Consider action of G on $\{X \in G : |X| = p^n\}$ by left mult.

---

we also showed $\longrightarrow$ $|G| = p^n \Rightarrow \forall\, k \leq n$, $\exists\, H_k \leq G$ $|H_k| = p^k$.

We use similarly the natural homomorphism.

21-373 11/4/2020

Def. Let p be prime, G is a p-group, provided $\forall a \in G$, $\exists n \in \mathbb{N}$, $|\langle a \rangle| = p^n$. Ex. $G = H_1 \times H_2$, where $H_1 = \mathbb{Z}/p\mathbb{Z}$, $H_2 = \mathbb{Z}/p^2\mathbb{Z}$. $|G| = p^3$, but $|\langle a \rangle| = p$ or p^2 only. (recall if $|G| = p^n$ then $Z(G) \neq \{1\}$)

(cyclic group) (direct products)

Prop. G is finite group, p is a prime.

G is a p-group $\Leftrightarrow \exists n$, $|G| = p^n$.

Proof. ($\Rightarrow$) o/w $\exists$ q prime $q \neq p$ and $q \mid |G|$. Using Cauchy $\exists H \leq G$

$|H| = q \Rightarrow \exists a \in H$ $\langle a \rangle = H$, so $|\langle a \rangle| = q$ contradicts that G is a p-group.

($\Leftarrow$) Suppose $n_0 \in \mathbb{N}$ s.t. $|G| = p^{n_0}$. Given $a \in G$ what is $|\langle a \rangle|$?

Let $H = \langle a \rangle$. As $H \leq G$ by Lagrange $|H| \mid |G| = p^{n_0}$, so $\exists n \leq n_0$ s.t. $|H| = p^n$.

Def. Let G be a group, $P \leq G$. P is called Sylow-p-subgroup of G provided

(1) P is a p-group for some prime p, and

(2) P is maximal: if H is p-group and $P \leq H \leq G$, then $H \leq P$

Theorem. Existence of Sylow p-groups.

Suppose G is finite, p is prime, $p \mid |G|$. Then $\exists P \leq G$

Proof. As $p \mid |G|$ there are $n, m \geq 1$ s.t. $|G| = p^n \cdot m$ where $(p, m) = 1$.

By Sylow's 1st Theorem, $\exists P \leq G$, $|P| = p^n$. Show this P is maximal. If o/w if $\exists Q \leq G$ also p-group, $Q \neq P$. By proposition $\exists k$ s.t. $|Q| = p^k > p^n$, contradicting $(p, m) = 1$, $|G| = p^n m$

2nd and 3rd Sylow's Theorems

inner automorphisms: $f_g(x) = gxg^{-1}$, $f_g \in \mathrm{Aut}(G)$

2nd. Let G be finite, P prime, $p \mid |G|$.

If $P, Q \leq G$ both Sylow-p-subgroups, then $\exists g \in G$, $Q = gPg^{-1}$

(all Sylow-p-subgroups are isomorphic)

Lemma. Suppose H is a finite p-group acting on a finite set S then $|S| \equiv |S_0| \bmod p$ where $S_0 = \{x \in S \mid \forall h \in H,\ hx = x\}$

Proof $S := \{xP \mid x \in G\}$. Q acts on S by left multiplication

$$g \in Q, \quad g \cdot (xP) = (gx)P$$

$$xP \in S_0 \iff \forall g \in Q \quad gxP = xP$$

$$x^{-1}gx \in P.$$

$$\iff x^{-1}Qx \subseteq P \Rightarrow x^{-1}Qx = P$$

Now since both P, Q are p-Sylow, $|P| = |Q| = p^n$ $\qquad Q = xPx^{-1}$.

$$|S| \equiv |S_0| \bmod p \Rightarrow |S| = [G : P],\ p \nmid [G : P] \Rightarrow |S_0| \not\equiv 0 \bmod p$$

$$\Rightarrow S_0 \neq \emptyset \Rightarrow \exists x_0 \text{ s.t. } x_0 P \in S_0$$

3rd Let G be finite, p prime, $p \mid |G|$. $S = \{P \leq G \mid P \text{ is Sylow } p\text{-subgroup}\}$.

Then $|S| \equiv 1 \bmod p$.

Proof. Fix $P \in S$.

By the previous theorem, $S = \{ gPg^{-1} : g \in G \}$.

$$|S| = [G : N_G(P)]$$
orbit stabilizer

Let P act on S by $\forall\, h \in P$, $h \cdot (gPg^{-1}) = h(gPg^{-1})h^{-1}$.

Fix Q, a Sylow p-subgroup. $Q \in S_0 \iff \forall x \in P \quad xQx^{-1} = Q$.

$\overset{\text{def.}}{\iff} P \leq N_G(Q)$ (squeeze P, Q inside $N_G(Q)$)

Clearly $Q \trianglelefteq N_G(Q)$. Since both P, Q are Sylow-p-subgroups of G, they are also Sylow-p-subgroups of $N_G(Q)$.

By 2nd Sylow, $\exists\, x \in N_G(Q)$ s.t. $P = xQx^{-1}$.

But $Q \trianglelefteq N_G(Q)$

so $xQx^{-1} = Q \Rightarrow P = Q$

So $S_0 = \{P\}$, so $|S_0| = 1$. By the congruence lemma,

$$|S| \equiv |S_0| \equiv 1 \bmod p.$$

Ex. Suppose G is finite, $H \leq G$. Then $G \neq \bigcup_{x \in G} xHx^{-1}$.

Consider the action of G on $S = \{G_1 \mid G_1 \leq G\}$ by conjugacy. $x \in G, G_1 \in S$.

$x \cdot G_1 := xG_1x^{-1}$.

[Fact: $\varphi: G \to H$ surjective homomorphism, $G_1 \leq G$ then $\varphi[G_1] \leq H$. In particular true when $\varphi = f_g$, $f_g(a) = gag^{-1}$.]

Now $\{xHx^{-1} \mid x \in G\} = \text{orbit}(H)$

$|\text{orbit}(H)| = [G : G_H]$

$= [G : N_G(H)]$

but $|xHx^{-1}| = |H|$. So $\left| \bigcup_{x \in G} xHx^{-1} \right| \leq [G : N_G(H)] \cdot |H| \leq G$.

($\leq$ for each x; $\leq [G:H]$)

in fact $\leq [G:H] \cdot (|H| - 1) + 1 < G$

Another proof of Sylow's 1st Theorem [$|G| = p^n \cdot m$, p is prime, $(p, m) = 1$. $\Rightarrow \exists P \leq G$, $|P| = p^n$.]

Proof. Case 1 Suppose G is abelian. By induction on n:

$n = 0$ Let $H = \{1\}$, $|H| = p^0 = 1$.

$n+1$ Suppose $|G| = p^{n+1} m$, where $(p, m) = 1$, G abelian.

By Cauchy, $\exists\, a \in G$, s.t. $|\langle a \rangle| = p$. Since G is abelian, all subgroups are normal. Let $G_1 = G/N$, $|G_1| = \frac{|G|}{|N|} = p^n \cdot m$.

By inductive hypothesis, $\exists\, H_1 \leq G_1$ of cardinality p^n. Let $H = \varphi^{-1}[H_1]$ where $\varphi: G \to G/N$ is the natural homomorphism

Case 2 - not abelian.

(conjugacy class eqn) $G = Z(G) \cup \bigcup_{a \in G - Z(G)} \text{whit}(a)$

$$\downarrow$$

$$|G| = |Z(G)| + \sum_{a \in G - Z(G)} [G : C_G(a)]$$

If $p \mid |Z(G)|$, then by Cauchy, take $a \in Z(G)$.

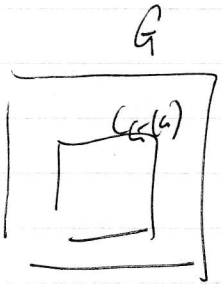
$|\underbrace{\langle a \rangle}_{N}| = p$, $N \trianglelefteq G$

$\varphi : G \to G$, homomorphism. $|G_1| = \frac{|G|}{|N|}$

Apply Inductive Hypothesis to find $H_1 \leq G_1$ of cardinality $\frac{p^{n+1} \cdot m}{p} = p^n \cdot m$

Fiber has $|\cdot| = p^{n+1}$.

Else, when $p \nmid |Z(G)|$.



$\exists\ a \in G - Z(G)$ s.t. $p \nmid [G : C_G(a)]$

By Lagrange, $|C_G(a)| = \frac{|G|}{[G : C_G(a)]} = \frac{p^{n+1} \cdot m}{[G : C_G(a)]}$

So $p^{n+1} \mid |C_G(a)|$.

fiber = pre image

As $a \notin Z(G) \Rightarrow C_G(a) \subsetneq G$.

$ha = ah$

$h = hah^{-1}$

So $|C_G(a)| < |G|$. → repeat, eventually get group cardinality p^{n+1}

Suppose instead we inducted on $|G|$. Then Apply Inductive Hypothesis to deduce that $C_G(a)$ contains a subgroup of order p^{n+1}.