Sylow Theorem

Date: Mar 13 Made by Eric

# Definitions and Theorems

**Definition 1.** *Let $G$ be a group, $X$ be a $G$-set, and $x \in X$*

*We call $O_x = \{gx | g \in G\}$ the* ***orbit*** *containing $x$*

**Definition 2.** $G_x = \{g \in G | gx = x\}$

**Definition 3.** $X_g = \{x \in X | gx = x\}$

**Definition 4.** $X_G = \{x \in X | \forall g \in G, gx = x\}$

**Definition 5.** *A group $G$ is a* ***p-group*** *if $\forall g \in G, ord(g) = p^q, \exists q \in \mathbb{N}$*

**Lemma 1.** *$G_x$ is a subgroup and $|O_x| = (G : G_x)$*

*Proof.* We now prove $G_x$ is a subgroup

$\forall g, h \in G_x, (gh)x = g(hx) = gx = x \implies gh \in G_x$ $G_x$ is closed under

$ex = x \implies e \in G_x$ Identity

$g \in G_x \implies gx = x \implies g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = ex = x \implies g^{-1} \in G_x$ Inverses

We now prove If the two elements $n, r$ are in the same left coset of $G_x$, $nx = rx$

$n^{-1}r \in G_x \iff n^{-1}rx = x \iff nx = rx$ done

Let $S = \{gG_x | g \in G\}$ be the set of left cosets of $H$ in $G$. By definition, $|S| = (G : G_x)$

We now prove the equation:

$$|O_x| = |S| = (G : G_x)$$

Let $\psi : O_x \to S$ be defined by $\psi(gx) = gH$ mapping

$\psi(nx) = \psi(rx) \implies nH = rH \implies nx = rx$ one-to-one

$\forall gH \in S, \psi(gx) = gH$ onto ■

**Corollary 1.1.** *Let $G$ be a finite group, and $X$ be a finite $G$-set.*

$|O_x| = \frac{|G|}{|G_x|}$

**Lemma 2.** *Let $G$ be a finite group, $X$ be a finite $G$-set, and $r$ denote the amount of orbits subset to $X$*

$r|G| = \sum_{g \in G} |X_g|$

*Proof.* $\sum_{g \in G} |X_g| = |\{(g,x)|gx = x\}| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|O_x|} = |G| \sum_{x \in X} \frac{1}{O_x} = |G|r$ ■

**Lemma 3.** *Let $p$ be a prime number, and $G$ be a finite $p$-group, and $X$ be a $G$-set.*

$$|X| \equiv_p |X_G|$$

*Proof.* Pick $\{x_1, x_2, \cdots, x_r\}$ from each orbits of $X$, where $|O_{x_i}| = 1 \iff 1 \leq i \leq n$

We now prove $|O_{x_i}| = 1 \iff x_i \in X_G$

$|O_{x_i}| = 1 \iff O_{x_i} = \{x_i\} \iff \forall g \in G, gx_i = x_i \iff x_i \in X_G$ done

We know $|X| = \sum_{i=1}^{r} |O_{x_i}| = \sum_{i=1}^{n} |O_{x_i}| + \sum_{i=n+1}^{r} |O_{x_i}| = |X_G| + \sum_{i=n+1}^{r} |O_{x_i}|$

We now prove $\sum_{i=n+1}^{r} |O_x| \equiv_p 0 \implies |X| \equiv_p |X_G|$

Let $i \geq n+1$

By Lemma 1, $|O_{x_i}| = \frac{|G|}{|G_{x_i}|}$
Because $G_{x_i}$ is a subgroup of $G$, for which $|G| = p^n$ and $|O_{x_i}| = \frac{|G|}{|G_{x_i}|} \neq 1$, so $|O_{x_i}| = \frac{|G|}{|G_{x_i}|} = p^k \equiv_p 0, \exists 0 < k \leq n$ done

■

**Theorem 4.** ***(If a prime divides the order of a group, then that group contain a cycilic subgroup of order p)*** *Let $p$ be a prime, and $p$ divides $|G|$.*

$$\textit{There exists an element } a \in G\textit{, such } ord(a) = p$$

*Proof.* Let $X = \{(g_1, g_2, \ldots, g_p)|g_1 g_2 \cdots g_p = e\}$

We now prove $|X| = |G|^{p-1} \implies |X| \equiv_p 0$

Arbitrarily filling random $g$ into $g_1, g_2, \ldots, g_{p-1}$ we see $(g_1, g_2, \ldots g_p) \in X \iff g_p = (g_1 g_2 \cdots g_{p-1})$

So There are $|G|^{p-1}$ distinct ways to construct elements in $X$ done

We now prove $\exists(a, a, \ldots, a) \in X$, where $a \neq e$, which give us $a^p = e \implies ord(a) = p$

Let $\psi : X \to X$ be defined by $\psi(g_1, g_2, \ldots g_p) = (g_p, g_1, g_2, \ldots g_{p-2}, g_{p-1})$

$\psi$ is well defined, since $g_p g_1 g_2 \cdots g_{p-2} g_{p-1} = (g_1 g_2 \cdots g_{p-1})^{-1}(g_1 g_2 \cdots g_{p-2} g_{p-1}) = e$

Because all $\psi$ do is simply moving every cordinates a slot after, $|\langle\psi\rangle| = p$

By Lemma 3, $0 \equiv_p |X| \equiv_p |X_{\langle\psi\rangle}|$

$e^p = e \implies (e, e, \ldots, e) \in X$

$\forall q \in \mathbb{Z}, \psi^q(e, e, \ldots, e) = (e, e, \ldots, e) \implies (e, e, \ldots, e) \in X_{\langle\psi\rangle}$

So, $|X_{\langle\psi\rangle}| > 0$

Because $0 \equiv |X_{\langle\psi\rangle}|$, so $\exists(a, a, \ldots, a) \in X_{\langle\psi\rangle} \subseteq X$, where $a \neq e$

$\blacksquare$

**Corollary 4.1.** *Let $G$ be a finite group. Then $G$ is a $p$-group if and only if $|G| = p^k, \exists k \in \mathbb{N}$*

*Proof.* $(\longleftarrow)$

$\forall g \in G, ord(g)$ divides $|G| = p^k \implies ord(g) = p^q, \exists 0 \leq q \leq k$

$(\longrightarrow)$

Assume $|G| = p^k r, \exists r \in \mathbb{N}$ such $p \not| r$

There exists a prime number $p_c \neq p$, such that $p_c | r$, so $p_c$ divides $|G|$

Then by Theorem 4, $\exists g \in G, ord(g) = p_c$ CaC $\blacksquare$

**Theorem 5.** *Let $G$ be a group, and $X = G$ (as a set), and be a $G$-set defined by $\forall g \in G, \forall x \in X, g(x) = gxg^{-1}$*

$$|G| = |Z(G)| + \textstyle\sum_{O_x \subseteq X, |O_x| > 1} |O_x|$$

*Proof.* We now prove $X$ is well defined

$\forall x \in X, g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$

$e(x) = exe^{-1} = x$ done

$|O_x| = 1 \iff O_x = \{x\} \iff \forall g \in G, g(x) = gxg^{-1} = x \iff gx = xg \iff x \in Z(G)$

$|G| = |X| = \sum_{O_x \subseteq X} |O_x| = |Z(G)| + \sum_{O_x \subseteq X, |O_x|>1} |O_x|$ ■

**Definition 6.** *$N[H] = \{g \in G | gHg^{-1} = H\}$ is the **normalizer** of $H$*

**Theorem 6.** *$N[H]$ is a subgroup of $G$, and $H \trianglelefteq N[H]$*

*Proof.* $\forall g_1, g_2 \in N[H], (g_1g_2)H(g_1g_2)^{-1} = g_1g_2Hg_2^{-1}g_1^{-1} = g_1Hg_1^{-1} = H \implies g_1g_2 \in N[H]$ $N[H]$ is closed under

$eHe^{-1} = H \implies e \in N[H]$

$\forall g \in N[H], g^{-1}Hg = g^{-1}(gHg^{-1})g = H \implies g^{-1} \in N[H]$ Inverses

$\forall g \in N[H], gHg^{-1} = H \implies H \trianglelefteq N[H]$

■

**Lemma 7.** *If $|H|$ is finite, then $\forall h \in H, ghg^{-1} \in H \implies g \in N[H]$*

*Proof.* $\forall h \in H, ghg^{-1} \in H \implies gHg^{-1} \subseteq H$

$|gHg^{-1}| = |H| < \infty \implies gHg^{-1} = H$ ■

Notice If $|H|$ is finite, $ghg^{-1} \in H \iff g \in N[H]$, but if $|H|$ is infinite, it may happen $ghg^{-1} \impliedby N[H]$ and $ghg^{-1} \not\longrightarrow g \in N[H]$

**Lemma 8.** *Let $H$ be a $p$-group of a finite group $G$. Then*

$$(N[H] : H) \equiv_p (G : H)$$

*Proof.* Let $S = \{gH \subseteq G | g \in G\}$

Let $S$ be a $H$-set defined by $h(gH) = (hg)H$

$S$ is well defined, since $\forall h_1, h_2 \in H, \forall gH \in S, h_1h_2(gH) = h_1(h_2gH) = h_1h_2gH = h_1h_2(gH)$ and $\forall gH \in S, e(gH) = egH = gH$

We now prove the equation:

$$(G : H) =_{\textbf{(i)}} |S| \equiv_p^{\textbf{(ii)}} |S_H| =_{\textbf{(iii)}} (N[H] : H)$$

**(i)** $S$ is the set of all left cosets of $H$.

**(ii)** $H$ is a $p$-group, clearly the order of $H$ is a power of p, so by Lemma 3, this is true.

**(iii)** Let $U = \{gH \subseteq G | g \in N[H]\}$

$\forall gH \in U, \forall h \in H, h(gH) = h(Hg) = Hg = gH \implies \forall gH \in U, gH \in S_H \implies U \subseteq S_H$

$\forall gH \in S_H, \forall h \in H, hgH = gH \implies \forall gH \in S_H, \forall h \in H, g^{-1}hgH = H \implies \forall gH \in S_H, \forall h \in H, g^{-1}hg \in H \implies \forall gH \in S_H, g \in N[H] \implies \forall gH \in S_H, gH \in U \implies S_H \subseteq U$

$\implies U = S_H$ ■

**Theorem 9.** *Let $G$ be a finite group, where $|G| = p^n m$, where $p \nmid m$ and $n \geq 1$*

*$G$ contains some subgroup of order $p^i$ of each $1 \leq i \leq n$, where the subgroup $H$ of order $p^i$, where $i < n$, is the normal subgroup of some subgroup of order $p^{i+1}$*

*Proof.* We prove by induction.

$$\text{Base step: } \exists H_1 \leq G, |H_1| = p^1$$

By Theorem 4, this is true.

$$\text{Induction step: } \exists H_i \leq G, |H_i| = p^i \implies \exists H_{i+1}, |H_{i+1}| = p^{i+1}$$

We now prove $p$ divides $|N[H_i]/H_i|$, so, by Theorem 4, there exists a subgroup $K \leq N[H_1]/H_1$ of order $p$

By Lemma 8, $(N[H_i] : H_i) \equiv_p (G : H_i) = p^{n-i}m \equiv_p 0$ **(Notice we only repeat to the case** $i = n - 1$**)**

Because $(N[H_i] : H_i) \geq 1$, so $p | (N[H_i] : H_i) = |N[H_i]/H_i|$ (done)

We now prove $\bigcup K \subseteq G$ is a subgroup of order $p^{i+1}$

$k_1, k_2 \in \bigcup K \implies k_1 H_1, k_2 H_2 \in K \implies (k_1 k_2) H_1 \in K \implies k_1 k_2 \in \bigcup K$

$e \in eH_1 = H_1 \in K \implies e \in \bigcup K$

$k_1 \in \bigcup K, k_1 H_1 \in K \implies k_1^{-1} H_1 \in K \implies k_1^{-1} \in \bigcup K$

$|\bigcup K| = |K||H_i| = pp^i = p^{i+1}$ (done)

We now prove $H_i \trianglelefteq \bigcup K$

$\forall k \in \bigcup K, kH_i \in K$, and $K \leq N[H_i]/H_i \implies kH_i \in N[H_i]/H_i \implies k \in N[H_i] \implies kH_i = H_i k$ (done)

■

**Theorem 10.** *Let $P_1$ and $P_2$ be two maximal p-subgroup of a finite group $G$*

$$\exists g \in G, gP_1 g^{-1} = P_2$$

*Proof.* Let $S = \{gP_1 | g \in G\}$, and let $S$ be a $P_2$-set defined by $\forall y \in P_2, \forall gP_1 \in S, y(gP_1) = (yg)P_1$

By Lemma 3, $P_2$ is a $p$-group $\implies |S| \equiv_p |S_{P_2}|$

Because $P_1$ is a maximal $p$-subgorup, $S$, as a collection of left-cosets of $P_1$, satisfy $|S| = m$, where $|G| = p^n m$ and $p \not| m$.

This give us $|S_{P_2}| \equiv_p |S| = m \not\equiv_p 0$

So $\exists gP_1 \in S_{P_2}, \forall y \in P_2, y(gP_1) = g(P_1) \implies g^{-1}ygP_1 = P_1 \implies g^{-1}yg \in P_1 \implies \exists gP_1 \in S_{P_2}, gP_2g = P_1$ ■

**Theorem 11.** *Let $G$ be a finite subgroup of order divided by prime $p$. Let $X = \{P_1, \ldots, P_n\}$ be the set of maximal $p$-subgroup of $G$*

$$|X| \equiv_p 1 \textit{ and } |X| \textit{ divides } |G|$$

*Proof.* Let $X$ be a $G$-set defined by $\forall g \in G, \forall P_i \in X, g(P_i) = gP_ig^{-1}$

We now prove $X$ is well defined

$\forall g \in G, \forall P_i \in X, \forall p, q \in g(P_i), p, q \in gP_ig^{-1} \implies p = gp_0g^{-1}, q = gq_0g^{-1}, \exists p_0, q_0 \in P_i \implies pq = gp_0g^{-1}gq_0g^{-1} = gp_0q_0g^{-1} \in gP_ig^{-1} = g(P_i)$

$\forall g \in G, \forall P_i \in X, e = geg^{-1} \in g(P_i)$

$\forall p \in g(P_i), p = gp_0g^{-1}, \exists p_0 \in P_i, \implies p^{-1} = gp_0^{-1}g^{-1} \in g(P_i)$ ($G$-action does send a maximal $p$-subgroup to another subgroup, of which we don't know the order yet)

Because $gpg^{-1} = gqg^{-1} \implies gp = gq \implies p = q$, so $|g(P_i) = gP_ig^{-1}| = |P_i| = p^n$, where $|G| = p^n m, \exists m : p \not| m \in \mathbb{N}$

Assume $g(P_i)$ is not a maximal $p$-subgroup, There is a $p$-subgroup $H$ properly containing $g(P_i)$, so $|H| = p^{n+k}, \exists k > 0$, this CaC to $|G| = p^n m$, since $|H| = p^{n+k}$ does not divide $|G| = p^n m$ (done)

We now prove $|X_{P_1}| = 1$, and since $P_1$ is a $p$-group, $|X| \equiv_p |X_{P_1}| = 1$

Let $P_i \in X_{P_1}$

$\forall p_1 \in P_1, p_1P_ip_1^{-1} = P_i \implies \forall p_1 \in P_1, p_1 \in N[P_i] \implies P_1 \leq N[P_i]$

$P_1$ and $P_i$ are obviously both maximal $p$-subgroup of $N[P_i]$, so by Theorem 9, $\exists g \in N[P_i], gP_ig^{-1} = P_1 \implies P_i = gP_ig^{-1} = P_1$

So $X_{P_1} = \{P_1\}$ (done)

We now prove $|X|$ divides $|G|$

By Theorem 10, every maximal $p$-group is conjugate to each other, so $|X|$ have only one orbit.

Then by Lemma 1, $|X| = |O_{P_1}| = (G : G_{P_1}) = \frac{|G|}{|G_{P_1}|}$ (done)

■

# Exercises