Application of 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. *Let $H, K \leq G$, $H \vee K$ is the smallest subgroup L satisfying $H \leq L$ and $K \leq L$*

Definition 6. *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.*

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

Theorem 2. *Every p-group G have a non-trivial center.*

Proof. $|G| = |Z(G)| + \sum_{|O_x|>1} |O_x|$

Let $n \in \mathbb{N}$, satisfy $p^n = |G|$

Because $\forall g \in G, ge = eg$, we know $e \in Z(G)$

Assume $Z(G)$ is trivial

$|Z(G)| = 1 \implies \sum_{|O_x|>1} |O_x| = |G| - 1 = p^n - 1$

$\forall x : |O_x| > 1, |O_x| = \frac{|G|}{|G_x|} = p^k$, where $k > 0$

Express $\sum_{|O_x|>1} |O_x|$ by polynomial $c_{n-1}p^{n-1} + c_{n-2}p^{n-2} + \cdots + c_1 p^1$

We see $p \not| p^n - 1$, yet $p| \sum_{|O_x|>1} |O_x| = |G| - 1 = p^n - 1$ CaC

∎

Theorem 3. ***(Second Isomorphism Theorem)*** *Let $N \trianglelefteq G$, and $H \leq G$. $HN/N \simeq H/(H \cap N)$*

Lemma 4. *Let $H \trianglelefteq G$ and $K \trianglelefteq G$. Let $H \cap K = \{e\}$ and $H \vee K = G$*

$$G \simeq H \times K$$

Proof. We now prove $H \vee K = HK$

$\forall hk \in HK, h \in H$ and $k \in K \implies hk \in H \vee K \implies HK \subseteq H \vee K$

We now prove HK is a subgroup

Because $H \trianglelefteq G$, so $\forall h_1k_1, h_2k_2 \in HK, \exists h_3 \in H, (h_1k_1)(h_2k_2) = h_1(h_3k_1(k_2 \in HK$

$e = ee \in HK$

$\forall hk \in HK, (hk)[(k^{-1}h^{-1}k^{-1})k] = e$ (done)

$\forall h \in H, h = he \in HK$, and $\forall k \in K, k = ek \in HK \implies H, K \in HK$

Because $H \vee K$ is the samllest subgroup of G containing H, K, so $H \vee K \subseteq HK$ (done)

By **Second Isomorphism Theorem**, we have $HK/K \simeq H/(H \cap K)$ and $HK/H \simeq K \simeq H/(H \cap K)$

Substituting $H \cap K = \{e\}$ and $HK = H \vee K = G$

We have $G/K \simeq H/\{e\} \simeq H$ and $G/H \simeq K/\{e\} \simeq K$, which give us $H \times K \simeq G/K \times G/H$

Now we prove $G \simeq G/K \times G/H \simeq H \times K$

Let $\phi : G \to G/K \times G/H$ be defined by $\phi(g) = (gK, gH)$

$\forall g_1, g_2 \in G, \phi(g_1)\phi(g_2) = (g_1K, g_1H)(g_2K, g_2H) = (g_1g_2K, g_1g_2H) = \phi(g_1g_2)$

$\phi(g_1) = \phi(g_2) \implies (g_1K, g_1H) = (g_2K, g_2H) \implies g_2^{-1}g_1K = K$ and $g_2^{-1}g_1H = H \implies g_2^{-1}g_1 \in K \cap H = \{e\} \implies g_2^{-1}g_1 = e \implies g_1 = g_2$

$HK = G \implies \forall g \in G, \exists h \in H, \exists k \in K, hk = g \implies \forall g \in G, \exists k \in K, \exists h \in H, gh = k$

Let $g_1, g_2 \in G$, and $g = g_2g_1^{-1}$. We pick $h \in H, k \in K$, such that $gh = k$

$g_1(g_1^{-1}h) \in H$

$g_2(g_1^{-1}h) = gh = k \in K$

So $\forall g_1, g_2 \in G, \exists g_3 \in G, g_1g_3 \in H, g_2g_3 \in K$

Then $\forall g_1, g_2 \in G, \exists g_3 \in G, g_1^{-1}g_3 \in H \implies g_1H = g_3H$ and $g_2^{-1}g_3 \in K \implies g_3K = g_2K$

So $\forall g_2K \in G/K, \forall g_1H \in G/H, \exists g_3 \in G, \phi(g_3) = (g_3K, g_3H) = (g_2K, g_1H)$ (done)

$\blacksquare$

Theorem 5. *Let p be a prime*

If a group G is of the order p^2, then G is abelian.

Proof. We split into two cases.

case 1: $\exists a \in G, \langle a \rangle = G$

$G = \langle a \rangle \implies G$ is cyclic $\implies G$ is abelian.

case 2: $\forall a \in G, \langle a \rangle \subset G$

Arbitrarily pick non-trivial $a \in G$, and let $b \in G \setminus \langle a \rangle$

Assume $a \in \langle b \rangle$

So, $\langle b \rangle = \langle a, b \rangle \subset G \implies |\langle b \rangle| = p$

Because $\forall a \in G, \langle a \rangle \subset G, |\langle a \rangle| = p = |\langle b \rangle|$, which give us $\langle a \rangle = \langle b \rangle$, since $a \in \langle b \rangle \implies \langle a \rangle \subseteq \langle b \rangle$

This CaC since we let $b \in G \setminus \langle a \rangle$, so $a \notin \langle b \rangle$

Let $S = \{a^n b^r | 1 \leq n \leq p, 1 \leq r \leq p\}$

We prove $\forall a^n b^r, a^{n'} b^{r'} \in S, a^n b^r = a^{n'} b^{r'} \implies n = n'$ and $r = r'$

If $r = r'$, then $a^n b^r = a^{n'} b^{r'} \implies a^n b^r = a^{n'} b^r \implies a^n = a^{n'} \implies n = n'$

Assume $r \neq r'$

Pick $q \in \mathbb{N} : q(r' - r) \equiv_p 1$

$\forall a^n b^r, a^{n'} b^{r'} \in S, a^n b^r = a^{n'} b^{r'} \implies a^{n-n'} = b^{r'-r}$

We see $a^{(n-n')q} = (b^{r'-r})^q = b^{q(r'-r)} = b$

This give us $b \in \langle a \rangle$ CaC to $b \in G \setminus \langle a \rangle$ (done)

BLUE enable us to count $|S| = p^2 = |G|$, where $S \subseteq G$. So $S = G$

$G = S \subseteq \langle a, b \rangle \subseteq G \implies \langle a, b \rangle = G$

By Theorem of Lagrange, $|\langle a \rangle| = 1$ or p or p^2, and also by Theorem of Lagrange, $|\langle b \rangle| = 1$ or p or p^2

$|\langle a \rangle| = 1 \implies \langle a \rangle = \{e\} \implies a = e \implies a \in \langle b \rangle$ CaC, so $|\langle a \rangle| \neq 1$

$|\langle a \rangle| = p^2 = |G| \implies \langle a \rangle = G$ CaC, so $|\langle a \rangle| = p$

Then by First Sylow Theorem, we know $\exists H \leq G, \langle a \rangle \trianglelefteq H$ and $|H| = p^2$

$|H| = p^2$ and $H \leq G \implies H = G$, so $\langle a \rangle \trianglelefteq G$

$|\langle b \rangle| = 1 \implies \langle b \rangle = \{e\} \implies b = e \implies b \in \langle a \rangle$ CaC, so $|\langle b \rangle| \neq 1$

$|\langle b \rangle| = p^2 = |G| \implies \langle b \rangle = G$ CaC, so $|\langle b \rangle| = p$

Then by First Sylow Theorem, we know $\exists H \leq G, \langle b \rangle \trianglelefteq H$ and $|H| = p^2$

$|H| = p^2$ and $H \leq G \implies H = G$, so $\langle b \rangle \trianglelefteq G$

Assume $\langle a \rangle \cap \langle b \rangle \neq \{e\}$, so $\exists 1 \leq n, r < p, a^n = b^r$

Pick $q \in \mathbb{N} : qr \equiv_p 1$

$a^n = (b^r)^q = b^q r = b \implies b \in \langle a \rangle$ CaC

Notice, in summary $\langle a \rangle \cap \langle b \rangle = \{e\}$, $G = S = \langle a \rangle \langle b \rangle$, $\langle a \rangle \trianglelefteq G$, and $\langle b \rangle \trianglelefteq G$

By Lemma 4, $G = \langle a \rangle \times \langle b \rangle = \mathbb{Z}_p \times \mathbb{Z}_p$, is abelian.

■

Theorem 6. *Let p and q be distinct primes with $p < q$, and G be a group with $|G| = pq$*

$$\exists H \leq G, |H| = q \text{ and } H \trianglelefteq G. \text{ Also } q \not\equiv_p 1 \implies G \text{ is cyclic}$$

Proof. Let k denote the number of Sylow q-subgroup of G

By Third Sylow Theorem, $k \equiv_q 1$ and $k|pq = |G|$

$k|pq \implies k = 1$ or p or q or pq

$k \equiv_q 1 \implies k = 1$

Let H denote the only Sylow q-subgroup.

By Second Sylow Theorem, $\forall g \in G, gHg^{-1} = H \implies H \trianglelefteq G$
Let r denote the number of Sylow p-subgroup of G

By Third Sylow Theorem, $r \equiv_p 1$ and $r|pq = |G|$

$r|pq \implies r = 1$ or p or q or pq

$r \equiv_p 1 \implies r = 1$ or q

If $q \not\equiv_p 1$, then $r \equiv_p 1$

Let H' denote the only Sylow p-subgroup.

By Second Sylow Theorem, $\forall g \in G, gH'g^{-1} \implies H' \trianglelefteq G$

Let $H = \langle a \rangle$ and $H' = \langle b \rangle$

Assume $H \cap H' \neq \{e\}$, so $\exists e \neq g \in G, g \in H \cap H'$

$g \in H \cap H' \implies n, r \in \mathbb{N} : g = a^n = b^r$

Pick $x \in \mathbb{N} : xr \equiv_p 1$

$a^{xn} = (a^n)^x = g^x = b^{rx} = b \implies b \in \langle a \rangle \implies \langle b \rangle \leq \langle a \rangle$, where $|\langle a \rangle| = q$ and $|\langle b \rangle|$ CaC to Theorem of Lagrange.

Let $S = \{a^r b^n | 1 \leq r \leq q, 1 \leq n \leq p\}$

We now prove $\forall a^n b^r, a^{n'} b^{r'} \in S, a^n b^r = a^{n'} b^{r'} \implies n = n'$ and $r = r'$

Assume $r \neq r'$

$a^{n-n'} = b^{r'-r}$

Pick $x \in \mathbb{N} : x(r'-r) \equiv_p 1$

$a^{x(n-n')} = (b^{r'-r})^x = b^{x(r'-r)} = b \implies b \in \langle a \rangle$ CaC

$r = r' \implies a^n = a^{n'} \implies n = n'$

BLUE enable us to count $|S| = pq = |G|$

$S \subseteq G \implies G = S$

To sum up, $\langle a \rangle \trianglelefteq G$, $\langle b \rangle \trianglelefteq G$, $\langle a \rangle \cap \langle b \rangle = \{e\}$ and $G = \langle a \rangle \langle b \rangle$

By Lemma 4, this give us $G = \langle a \rangle \times \langle b \rangle = \mathbb{Z}_q \times \mathbb{Z}_p = \mathbb{Z}_{pq}$

∎

Theorem 7. *Let H and K be two finite subgroup of a group G*

$$|HK| = \frac{(|H|)(|K|)}{|H \cap K|}$$

Proof. Let $t = |H \cap K|$

In $H \times K$, we let $(h, k) \sim (h', k')$ if $hk = h'k'$

We now prove $\sim$ is an equivalence relation

Clearly, $\forall (h, k) \in H \times K, (h, k) \sim (h, k)$

$(h, k) \sim (h', k') \implies hk = h'k' \implies (h', k') \sim (h, k)$

$(h, k) \sim (h', k')$ and $(h', k') \sim (h'', k'') \implies hk = h'k'$ and $h'k' = h''k'' \implies hk = h''k'' \implies (h, k) \sim (h'', k'')$ (done)

Let $\psi : HK \to H \times K / \sim$, defined by $\psi(hk) = [(h, k)]$

ψ is well defined since $hk = h'k' \implies (h, k) \sim (h', k')$

ψ is one-to-one, since $\psi(hk) = \psi(h'k') \implies (h, k) \sim (h', k') \implies hk = h'k'$

ψ is clearly onto.

So $\psi : HK \to H \times K / \sim$ is one-to-one and onto.

We now prove $\forall h_1k_1 \in HK, \exists!\{h_1, \ldots, h_t\}, \{k_1, \ldots, k_t\}, |\{h_1, \ldots, h_t\}| = t = |\{k_1, \ldots, k_t\}|$ and $h_1k_1 = h_2k_2 = \cdots = h_tk_t$, which tell us in each equivalent classes of $H \times K$, there is exactly t number amount of elements.

Let $\{e = a_1, \ldots, a_t\} = H \cap K$

For each $1 \leq i \leq t$, we pick $h_i = h_1a_i$ and $k_i = a_i^{-1}k_1$

Assume there exists $h_{t+1}k_{t+1} = h_1k_1$

$h_1^{-1}h_{t+1} = k_1k_{t+1}^{-1} \in H \cap K \implies \exists a_i \in H \cap K, h_{t+1} = h_1a_i$ and $k_{t+1} = a_i^{-1}k_1 \implies h_{t+1} = h_i$ and $k_{t+1} = k_i$ CaC (done)

Then $|HK| = |H \times K/\sim| = \frac{|H||K|}{t} = \frac{|H||K|}{|H\cap K|}$

■

Theorem 8. *No group of order* 30 *is simple*

Proof. Let G be a group of order 30

By Sylow First Theorem, we know there exists at least a Sylow 3-subgroup and a Sylow 5-subgroup of G

Let S_3 be the set of all Sylow 3-subgroup, and S_5 be the set of all Sylow 5-subgroup

By Sylow Third Theorem, we know $|S_3| \equiv_3 1$ and $|S_3|$ divides 30, which give us $|S_3| = 1$ or 10

By Sylow Third Theorem, we know $|S_5| \equiv_5 1$ and $|S_5|$ divides 30, which give us $|S_5| = 1$ or 6

Assume $|S_3| = 10$ and $|S_5| = 6$

We now prove $\forall H, K \in S_3, H \neq K \implies H \cap K = \{e\}$

Write $H = \langle a \rangle$, and $K = \langle b \rangle$

Assume $\exists i \neq 0, b^i \in \langle a \rangle$

Notice $\forall i \neq 0, \langle b \rangle = \langle b^i \rangle$, since $|\langle b \rangle| = 3$, which is a prime

For each $i \neq 0, b^i \in \langle a \rangle \implies \langle b^i \rangle \in \langle a \rangle \implies \langle b \rangle \in \langle a \rangle$, where $|\langle b \rangle| = 3 = |\langle a \rangle|$, so $H = \langle b \rangle = \langle a \rangle = K$ CaC

So $\forall i \neq 0, b^i \notin \langle a \rangle = H$

Every element in $H \cap K$ is in K, so we can express each element in $H \cap K$ in the form of $b^i, \exists i \in \mathbb{Z}$

This give us $b^i \in K \cap H \implies i = 0 \implies b^i = e$ (done)

So we see $\bigcup S_3$ contains $2 * 10$ distinct elements of G of order 3

We now prove $\forall H, K \in S_5, H \neq K \implies H \cap K$

Write $H = \langle a \rangle$, and $K = \langle b \rangle$

Assume $\exists i \neq 0, b^i \in \langle a \rangle$

Notice $\forall i \neq 0$, $\langle b \rangle = \langle b^i \rangle$, since $|\langle b \rangle| = 5$, which is a prime

For each $i \neq 0$, $b^i \in \langle a \rangle \implies \langle b^i \rangle \in \langle a \rangle \implies \langle b \rangle \in \langle a \rangle$, where $|\langle b \rangle| = 5 = |\langle a \rangle|$, so $H = \langle b \rangle = \langle a \rangle = K$ CaC

So $\forall i \neq 0, b^i \notin \langle a \rangle = H$

Every element in $H \cap K$ is in K, so we can express each element in $H \cap K$ in the form of $b^i, \exists i \in \mathbb{Z}$

This give us $b^i \in K \cap H \implies i = 0 \implies b^i = e$ (done)

So we see $\bigcup S_5$ contains $4 * 6$ distinct elements of G of order 5

The 20 distinct elements of order 3 in $\bigcup S_3$ and the 24 distinct element of order 5 in $\bigcup S_5$ are all distinct, because an element can not be both order 3 and 5

So there exists at least 44 distinct elements of order 3 or 5, in a group of order 30 CaC

So $|S_3| = 1$ or $|S_5| = 1$

$|S_3| = 1$ or $|S_5|$ indicate there exists only one Sylow 3-subgroup, or there exists only one Sylow 5-subgroup

By Second Sylow Theorem, we know if there exists only one Sylow p-subgroup H of G, then $\forall g \in G, gHg^{-1} = H$, which give us $H \trianglelefteq G$

■

Theorem 9. *No group of order* 48 *is simple*

Proof. Let G be a group of order 48

Assume G is simple, that is, G have no normal subgroups

By First Sylow Theorem, we know there exists a Sylow 2-subgroup of G of order 16

Let S_{16} be the set of all Sylow 2-subgroup

By Third Sylow Theorem, we know $|S_{16}| \equiv_2 1$ and $|S_{16}|$ divides 48

So $|S_{16}| = 1$ or 3

Assume $|S_{16}| = 1$

Let $S_{16} = \{H\}$

$\forall g \in G, gHg^{-1} \in S_{16} \implies \forall g \in G, gHg^{-1} = H \implies H \trianglelefteq G$ CaC

So $|S_{16}| = 3$

Write $S = \{H, K, L\}$

We now prove $H \cap K \trianglelefteq G$

$H \cap K \leq H \implies |H \cap K| = 1, 2, 4, 8, 16$

Assume $|H \cap K| = 1$ or 2 or 4

$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{16^2}{1,2,4} > 48 = |G|$ CaC

Assume $|H \cap K| = 16$

$|H| = |K| = |H \cap K| = 16 \implies H = K$ CaC

So $|H \cap K| = 8$

This give us $(H : H \cap K) = 2 = (K : H \cap K)$

So $H \cap K \trianglelefteq H$ and $H \cap K \trianglelefteq K$

So $H \leq N[H \cap K]$

This give us $|N[H \cap K]| = 16$ or 48

Assume $|N[H \cap K]| = 16$

Then $H \leq N[H \cap K] \implies N[H \cap K] = H$ CaC to $H \cap K \trianglelefteq K$, since we can pick an element in K, that is not in H, but is in $N[H \cap K]$

So $|N[H \cap K]| = 48 = |G|$, which give us $N[H \cap K] = G$ (done) ■

Theorem 10. *No group of order* 36 *is simple*

Proof. Let G be a group of order 36

Assume G is simple

By Sylow First Theorem, we know there exists some 3-subgroup of order 9

Let S_9 be the set of all Sylow 3-subgroup

By Sylow Third Theorem, we know $|S_9| \equiv_3 1$ and $|S_9|$ divides 36

So $|S_9| = 1$ or 4

Assume $|S_9| = 1$

The only element, here we denote H_0, of S_9 is a normal subgroup of G, since by Sylow Second Theorem, $\forall g \in G, gH_0g^{-1} \in S_9 \implies gH_0g^{-1} = H_0$ CaC

So $|S_9| = 4$

Write $\{S_9\} = \{H, K, L, M\}$

We now prove $|H \cap K| = 3$

Because $H \cap K \leq H$, where $|H| = 9$, $|H \cap K| = 1$ or 3 or 9

Assume $|H \cap K| = 1$

$|HK| = \frac{|H||K|}{|H \cap K|} = 81 > 36 = |G|$ CaC

Assume $|H \cap K| = 9$

$|H \cap K| = 9 = |H| \implies H \cap K = H \implies H \subseteq K$ CaC (done)

We now prove $|N[H \cap K]| = 9$ or 18 or 36

$|H \cap K| = 3 \implies H \cap K$ is a 3-group

So we have $(N[H \cap K] : H \cap K) \equiv_3 (G : H \cap K) = 12 \equiv_3 0$

Then $3 | \frac{|N[H \cap K]|}{|H \cap K|}$

So 9 divides $|N[H \cap K]|$

This give us $|N[H \cap K]| = 9$ or 18 or 36 (done)

We now prove $|N[H \cap K]| = 18$ or 36

Assume $|N[H \cap K]| = 9$

Notice $|H| = |K| = 9 = 3^2$, by Theorem 5, indicate that H and K are all abelian groups, so $H \cap K \trianglelefteq H$ and K

Then, $H \cup K \subseteq N[H \cap K]$, so $N[H \cap K] \geq 9 + 9 - 3 = 15 > 9$ CaC (done)

If $|N[H \cap K]| = 18$, $(G : N[H \cap K]) = 2$, which give us $N[H \cap K] \trianglelefteq G$

If $|N[H \cap K]| = 36 = |G|$, then $N[H \cap K] = G$, which give us $H \cap K \trianglelefteq G$ ■

Theorem 11. *If a group G is of order $(3)(5)(17)$, then $G \simeq \mathbb{Z}_{(3)(5)(17)}$*

Proof. We now prove there exists a subgroup H of G of order 17, such that G/H is abelian and cyclic

By First Sylow Theorem, we know there exists some 17-subgroup of G of order 17

Let S_{17} be the set of all Sylow 17-subgroup of G

By Third Sylow Theorem, we know $|S_{17}| \equiv_{17} 1$ and $|S_{17}|$ divides $(3)(5)(17)$

This give us $|S_{17}| = 1$

We write $S_{17} = \{H\}$

So $H \trianglelefteq G$, and we see $|G/H| = (3)(5)$, where $5 \not\equiv_3 1$

By Theorem 6, G/H is abelian and cyclic (done)

Let C be the commutator subgrouop of G

We now prove G/N is abelian $\iff C \leq N$

$\forall aN, bN \in G/N, aNbN = bNaN \iff abN = baN \iff a^{-1}b^{-1}abN = N \iff a^{-1}b^{-1}ab \in N$ (done)

So we know $C \leq H$, where $|H| = 17$

This give us $|C| = 1$ or 17

We now prove $|C| = 1$

By First Sylow Theorem, we know there exists some 3-subgroup of G of order 3

Let S_3 be the set of all Sylow 3-subgroup of G

By Third Sylow Theorem, we know $|S_3| \equiv_3 1$ and $|S_5|$ divides $(3)(5)(17)$

This give us $|S_3| = 1$

We write $S_3 = \{H_1\}$

So $H_1 \trianglelefteq G$, and we see $|G/H_1| = (5)(17)$, where $17 \not\equiv_5 1$

By Theorem 6, G/H_1 is abelian and cyclic

So $C \leq H_1$, where $|H_1| = 3$, which give us $|C| = 3$ or 1 (done)

So $C = \{e\}$, which give us $G \simeq G/C$ is abelian , since $C \leq C$ ■

Exercises

4.

Prove that every group G of order $(5)(7)(47)$ is abelian and cyclic

Proof. We first prove There exist a 5-subgroup H of G, of order 5 and a 7-subgroup K of G, of order 7, where $H \trianglelefteq G$, and $K \trianglelefteq G$

By First Sylow Theorem, there exists some 5-subgroups of order 5

Let S_5 be the set of all Sylow 5-subgroup of G

By Third Sylow Theorem, $|S_5| \equiv_5 1$ and $|S_5|$ divides $(5)(7)(47)$

$7 \equiv_5 2 \equiv_5 47$ so $|S_5| = 1$

Write $S_5 = \{H\}$

By Second Sylow Theorem, $\forall g \in G, gHg^{-1} \in S_5$, so $\forall g \in G, gHg^{-1} = H$, which give us $H \trianglelefteq G$

By First Sylow Theorem, there exists some 7-subgroups of order 7

Let S_7 be the set of all Sylow 7-subgroup of G

By Third Sylow Theorem, $|S_7| \equiv_5 7$ and $|S_7|$ divides $(5)(7)(47)$

$5 \not\equiv_7 1$ and $47 \equiv_7 5 \not\equiv_7 1$ and $(5)(47) \equiv_7 4 \not\equiv_7 1$ so $|S_7| = 1$

Write $S_7 = \{K\}$

By Second Sylow Theorem, $\forall g \in G, gKg^{-1} \in S_5$, so $\forall g \in G, gKg^{-1} = K$, which give us $K \trianglelefteq G$ (done)

Let C be the commutator subgroup of G

We prove $C \leq H$ and $C \leq K$

$|G/H| = (7)(47)$, where $47 \not\equiv_7 1$, give us G/H is abelian

So $C \leq H$

$|G/K| = (5)(47)$, where $47 \not\equiv_5 1$, give us G/K is abelian

So $C \leq K$ (done)

Because $|H| = 5$ is co-prime to $|K| = 7$

So $|C|$ can only be 1, which give us $C = \{e\}$

Then $G \simeq G/C$ is abelian

So $G \simeq \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{47} \simeq \mathbb{Z}_{(5)(7)(47)}$ ∎

5.

Prove that no group of order 96 is simple

Proof. Let G be a group of order 96

Assume G is simple

$96 = (32)(3)$

By First Sylow Theorem, there exists some Sylow 2-subgroup of order 32

Let S_2 be the set of all Sylow 2-subgroup

By Third Sylow Theorem, $|S_2| \equiv_2 1$ and $|S_2|$ divides 96

So $|S_2| = 1$ or 3

Assume $|S_2| = 1$

Write $S_2 = \{H\}$

By Second Sylow Theorem, $\forall g \in G, gHg^{-1} \in S_2$, so $\forall g \in G, gHg^{-1} = H$ CaC

So $|S_2| = 3$

Write $S_2 = \{H, K, L\}$

$H \cap K \leq H \implies |H \cap K| = 1$ or 2 or 4 or 8 or 16 or 32

Assume $|H \cap K| \leq 8$

$|HK| = \frac{|H||K|}{|H \cap K|} \geq (32)(4) > 96 = |G|$ CaC

Assume $|H \cap K| = 32$

$H \cap K \leq H$, where $|H \cap K| = 32 = |H|$, give us $H \cap K = H$

So $H \subseteq K$ CaC

$|H \cap K| = 16 \implies (H : H \cap K) = 2 = (K : H \cap K) \implies H \cap K \trianglelefteq H$ and $H \cap K \trianglelefteq K$

So $H \cup K \subseteq N[H \cap K]$, and $H \leq N[H \cap K]$

$H \leq N[H \cap K] \implies |N[H \cap K]|$ is divided by $|H|$

So $|N[H \cap K]| = 32$ or 96

Assume $|N[H \cap K]| = 32$

$H \leq N[H \cap K]$, where $|H| = 32 = |N[H \cap K]|$, give us $N[H \cap K] = H$

Then $K \subseteq N[H \cap K] = H$, given by $H \cap K \trianglelefteq K$ CaC

Then $|N[H \cap K]| = 96 = |G|$

So $N[H \cap K] = G$, which give us $H \cap K \trianglelefteq G$ CaC

■

6.

Prove that no group of order 160 is simple

Proof. Let G be a group of order 160

Assume G is simple

We now prove there is 32 distinct Sylow 5-subgroup

$160 = (32)(5)$

By First Sylow Theorem, there exists some Sylow 5-subgroup of order 5

Let S_5 be the set of all Sylow 5-subgroup

By Third Sylow Theorem, $|S_5| \equiv_5 1$ and $|S_5|$ divides $|G| = 160$

This give us $|S_5| = 1$ or 32

Assume $|S_5| = 1$

Write $S_5 = \{H_0\}$

By Second Sylow Theorem, $\forall g \in G, gH_0g^{-1} \in S_5$

So $\forall g \in G, gH_0g^{-1} = H_0$ CaC (done)

We now prove there exists 5 distinct Sylow 2-subgroup of order 32

By First Sylow Theorem, there exists some Sylow 2-subgroup of order 32

Let S_2 be the set of all Sylow 2-subgroup

By Third Sylow Theorem, we know $|S_2| \equiv_2 1$ and $|S_2|$ divides $160 = |G|$

So $|S_2| = 1$ or 5

Assume $|S_2| = 1$

Write $S_2 = \{H_1\}$

By Third Sylow Theorem, we know $\forall g \in G, gH_1g^{-1} \in S_2$

So $\forall g \in G, gH_1g^{-1} = H_1$ CaC (done)

Notice there are 32 distinct Sylow 5-subgroup of order 5

This tell us that there are $4 * 32$ distinct element of order 5

which lead us to that there are only $32 = 160 - 32 * 4$ elements can consist only one distinct Sylow 2-subgroup of order 32 CaC

$\blacksquare$