Department of Mathematics
Guru Nanak Dev University, Amritsar-143005
Notes on 'Sylow's theorems & assignment #4

Abstract

We discuss the Sylow's theorems and their applications.

0.1 Sylow's theorems

Lemma 0.1. *If p is a prime and r and m be positive integers such that p^r divides m but p^{r+1} does not divide m then p^{r+1} does not divide ${}^{p^\alpha m}C_{p^\alpha}$ for all positive integers α.*

Proof. We have

$$\begin{aligned} {}^{p^\alpha m}C_{p^\alpha} &= m\frac{(p^{\alpha m}-1)\cdots(p^\alpha m-(p^\alpha-1)}{(p^\alpha-1)\cdots(p^\alpha-(p^\alpha-1))} \\ &= m\prod_{i=1}^{p^\alpha-1}\frac{p^\alpha m-i}{p^\alpha-i}. \end{aligned} \tag{0.1}$$

Note that for each i the highest power of p that divides $p^\alpha m-i$ and $p^\alpha-i$ is same therefore factors out of $\prod_{i=1}^{p^\alpha-1}\frac{p^\alpha m-i}{p^\alpha-i}$ and p does not divide this product. Hence from Eq. (0.2) we see that highest power of p dividing ${}^{p^\alpha m}C_{p^\alpha}$ and m is the same. The assertion follows now. □

Definition: (Sylow$-p-$subgroup) Let G be a finite group and p be a prime such that p^α divides $|G|$. Then a subgroup of G of order p^α is called a $p-$subgroup of G. A $p-$subgroup of order p^α such that $p^{\alpha+1}$ does not divide $|G|$, is called a Sylow$-p-$subgroup of G.

Theorem 0.2. Sylow's theorems

Sylow's 1st theorem. *Let G be a finite group of order n. If p is a prime such that p^α divides n for some positive integer α then G has a subgroup of order p^α.*

Sylow's 2nd theorem. *Any two Sylow-p-subgroups of G are conjugates.*

Sylow's 3rd theorem. *The number n_p of Sylow$-p-$subgroups of G satisfies the following.*

$$n_p \text{ divides } [G:N_G(H)],\ n_p \equiv 1 \mod p.$$

where H denotes a Sylow$-p-$subgroup of G.

Proof. **Sylow's 1st theorem.** Let $|G| = p^\alpha m$ and r be a positive integer such that p^r divides m but p^{r+1} does not divide m. Let $\mathcal{M}$ be the set of all subsets of G each having p^α elements. Then

$$|\mathcal{M}| = {}^{p^\alpha m}C_{p^\alpha}$$

and under the action of G on set $\mathcal{M}$ defined by

$$g \bullet M = gM,$$

$\mathcal{M}$ is equal to disjoint union of its orbits. With this we obtain

$${}^{p^\alpha m}C_{p^\alpha} = |\mathcal{M}| = \sum_{M\in\mathcal{M}}|\mathcal{O}_M| = \sum_{M\in\mathcal{M}}\frac{|G|}{|\mathrm{Stab}(M)|}.$$

By preceding lemma 0.1 highest power of p dividing $\sum_{M\in\mathcal{M}}\frac{|G|}{|\mathrm{Stab}(M)|}$ is p^r. Therefore, there must be one term in this summation which is not divisible by p^{r+1}. Let this corresponds to $M_1 \in \mathcal{M}$. Define $H := \mathrm{Stab}(M_1) \leq G$. we will prove that $|H| = p^\alpha$. Since $|G| = |\mathcal{O}_{M_1}||H|$, and that highest power of p dividing $|G|/|\mathcal{O}_{M_1}|$ is p^α, it follows that $|H| \geq p^\alpha$. For reverse inequality, fix a $m \in M_1$ then

$$Hm := \{xm, x \in G \mid x \bullet M_1 = xM_1 = M_1\} \subseteq M_1$$

since each element of Hm is of the form $xm \in xM_1 = M_1$ i.e. $xm \in M_1$. Therefore

$$|H| = |Hm| \leq |M_1| = p^\alpha.$$

Thus we have proved that G has a subgroup H such that $|H| = p^\alpha$.

Sylow's 2nd theorem. Let A and B be two distinct Sylow$-p-$subgrops of G such that $|A| = |B| = p^r$ such that p^{r+1} does not divide $|G|$. Define a set $X := \{AxB \mid x \in G\}$ where $AxB := \{axb \mid a \in A,\ b \in B\}$. Then under the action of G on X defined by

$$g \bullet (AxB) := A(gx)B$$

[1]E-mail: sonumaths@gmail.com; Web page: https://sites.google.com/site/sonumaths2/

X is equal to disjoint union of orbits in X. Since highest power of p dividing $|G|$ is r, it follows that there is at least one $x \in G$ for which p^{r+1} does not divide $|\mathcal{O}_{AxB}|$. As $\mathcal{O}_{AxB} = X$ and $\text{Stab}(AxB) := \{g \in G \mid AgxB = AxB\} = AxBx^{-1}$, we have

$$|G| = |\mathcal{O}_{AxB}||\text{Stab}(AxB)| = |X|\frac{|A||xBx^{-1}|}{|A \cap xBx^{-1}|}$$

Since $|A| = p^r = |B|$ therefore $|A \cap xBx^{-1}| = p^\alpha$ for some nonnegative integer $\alpha < r$. We see that

$$|G| = |X|p^{2r-\alpha}.$$

It follows that $2r - \alpha \leq r$ or $r \leq \alpha$ which is possible only when $\alpha = r$. Hence $|A \cap xBx^{-1}| = p^r = |A|$ which implies that $A \cap xBx^{-1} = A$ or $A \subseteq xBx^{-1}$ i.e. $A = xBx^{-1}$. This proves that A is conjugate to B.

Sylow's 3rd theorem. Let H be a Sylow$-p-$subgroup of G of order p^r. Define $Y := \{xHx^{-1} \mid x \in G\}$ as the set of all conjugates of H in G which by Sylow's 2nd theorem, consists of all the Sylow$-p-$subgroups of G. Under the action of G on the set Y defined by

$$g \bullet (xHx^{-1}) := g(xHx^{-1})g^{-1} = (gx)H(gx)^{-1}$$

$$|G| = |\mathcal{O}_H||\text{Stab}(H)| = |Y||N_G(H)|$$

from which it follows that

$$|Y| = [G : N_G(H)].$$

For the remaining part we consider the action of the group $H \times H$ on G defined by

$$(h_1, h_2) \bullet x = h_1 x h_2^{-1}.$$

Under this action, for any $x \in G$,

$$\mathcal{O}_x = \{h_1 x h_2^{-1} \mid h_1, h_2 \in H\} = HxH.$$

Also note that for $x \in N_G(H)$, $\mathcal{O}_x = HxH = xH$ which is a left coset of H in $N_G(H)$. We have

$$\begin{aligned} |G| = \sum_{x \in G} |\mathcal{O}_x| &= \sum_{x \in N_G(H)} |xH| + \sum_{x \notin N_G(H)} |HxH| \\ &= |N_G(H)| + \sum_{x \notin N_G(H)} |HxHx^{-1}| \end{aligned} \tag{0.2}$$

since $\sum_{x \in N_G(H)} |xH| = |N_G(H)|$ and the map $hxh' \mapsto hxh'x^{-1}$ is a bijection i.e. $|HxH| = |HxHx^{-1}|$. Hence we see that

$$|G| = |N_G(H)| + \sum_{x \notin N_G(H)} \frac{|H||xHx^{-1}|}{|H \cap xHx^{-1}|}$$

$$= |N_G(H)| + \sum_{x \notin N_G(H)} p^{2r-\alpha}$$

where $|H \cap xHx^{-1}| = p^\alpha$ for some $\alpha < r$ since $H \neq xHx^{-1}$. Also as $H \leq N_G(H)$ the highest power of p dividing $|N_G(H)|$ is p^r. Consequently

$$\sum_{x \notin N_G(H)} p^{2r-\alpha} = kp^{r+1}$$

for some positive integer k and

$$\frac{|G|}{|N_G(H)|} = n_p = 1 + \frac{kp^{r+1}}{|N_G(H)|} \equiv 1 \mod p.$$

This completes the proof. □

Remark: 2nd part of the Sylow's 3rd theorem can be proved using action of $N_G(H)$ on the set Y via conjugation i.e.

$$s \bullet (xHx^{-1}) = (sx)H(sx)^{-1}.$$

Then $\mathcal{O}_{xHx^{-1}} = \{(sx)H(sx)^{-1} \mid s \in N_G(H)\} = H$ if $x \in N_G(H)$. Also $\text{Stab}(xHx^{-1}) = \{s \in N_G(H) \mid s \bullet (xHx^{-1}) = s(xHx^{-1})s^{-1} = xHx^{-1}\} = N_{N_G(H)}(xHx^{-1}) = N_G(H) \cap N_G(xHx^{-1})$. Therefore

$$n_p = |Y| = 1 + \sum_{x \notin N_G(H)} \frac{|N_G(H)|}{|N_G(H) \cap N_G(xHx^{-1})|}$$

$$\text{or} \quad n_p \equiv 1 \mod p$$

where we now show that each term under the summation is divisible by p. We first claim that for all $x \in G - N_G(H)$, $H \nsubseteq N_G(xHx^{-1})$ otherwise if $H \subseteq N_G(xHx^{-1})$ then $HxHx^{-1}$ is a subgroup of G where p^{r+1} divides $|HxHx^{-1}|$ which is a contradiction. Similarly $xHx^{-1} \notin N_G(H)$. Therefore highest power of p dividing $|N_G(H) \cap N_G(xHx^{-1})|$ is $\leq p^{r-1}$ where as $p^r = |H|$ divides $|N_G(H)|$. Consequently p divides $\frac{|N_G(H)|}{|N_G(H) \cap N_G(xHx^{-1})|}$.

0.2 Applications

> I have always grown from my problems and challenges, from the things that don't work out. That's when I have really learned!
>
> **–Carol Burnett**

Remark: Note that for a finite group G if H is a Sylow$-p-$subgroup of G then

$$n_p = \frac{|G|}{|N_G(H)|} = \frac{|G|}{|H|}\frac{|H|}{|N_G(H)|}$$

which gives

$$\frac{|G|}{|H|} = n_p \frac{|N_G(H)|}{|H|}.$$

It follows that $\boxed{n_p \textbf{ always divides } \frac{|G|}{|H|}.}$

Proposition 0.3. (Cauchy theorem) *If p is a prime divisor of order of a finite group G then G has an element of order p.*

Proof. Using Sylow's 1st theorem for every prime power $p^\alpha,\ \alpha = 1, 2, ...$ dividing $|G|$, G has a subgroup of order p^α, in particular take $\alpha = 1$ such that p divides $|G|$ and therefore G has a subgroup H of order p. Then H is cyclic and generator of H is an element of G of order p. □

Proposition 0.4. *A Sylow$-p-$subgroup H_p is normal if and only if it is unique subgroup of order $|H_p|$ i.e. $n_p = 1$.*

Proof. By Sylow's second theorem, any two Sylow$-p-$subgroups are conjugates, therefore $H_p \trianglelefteq G$ if and only if H_p contains its every conugate i.e. there is exactly one Sylow$-p-$subgroup of G. □

Example: (Groups of order pq where $p < q$). Let $|G| = pq$ for some distinct primes p and q, $(p < q)$. Let P is a Sylow$-p-$subgroup of G and Q be a Sylow$-q-$subgroup. We show that $Q \trianglelefteq G$. Using proposition 0.4 we just need to show that $n_q = 1$. As n_q divides $[G : H] = p$ therefore either $n_q = 1$ or $n_q = p$ since $n_q \equiv 1 \mod q$ and $1 < p < q$ it follows that $p \not\equiv 1 \mod q$ therefore the only possibility is $n_q = 1$.
Similarly n_p divides q therefore $n_p = 1$ or q. If $q \not\equiv 1$ then $n_p = 1$ hence $P \trianglelefteq G$ and therefore $PQ \leq G$. First observe that $P \cap Q = \{1\}$ since $p < q$, and $|PQ| = |P||Q| = pq = |G|$ thus $PQ = G$. We will show that G is abelian. If $x \in P$ and $y \in Q$, consider the element $xyx^{-1}y^{-1}$ we have $P \ni \underbrace{x}_{\in P}\underbrace{yx^{-1}y^{-1}}_{\in P\cdot\because P\trianglelefteq G} = \underbrace{xyx^{-1}}_{\in Q\cdot\because Q\trianglelefteq G}\underbrace{y^{-1}}_{\in Q} \in Q$. It follows that $xyx^{-1}y^{-1} \in (P \cap Q) = \{1\}$, therefore $xyx^{-1}y^{-1} = 1$ or $xy = yx$. We have proved that PQ hence G is abelian. Since P and Q are cyclic let $P = \langle x\rangle$ and $Q = \langle y\rangle$. Then it directly follows that $(xy)^{pq} = 1$ i.e. $|xy| = pq$. This proves that G is cyclic.
If p divides $q - 1$ then we will show later that there is unique-nonabelian group G of order pq with $n_p = q$.

Example: (Groups of order 30). Let G be a group of order $30 = 2\times3\times5$. We will show that G is not simple. Let P be Sylow$-5-$subgroup and Q be Sylow$-3-$subgroup of G. If any of P or Q is normal then we have nothing to prove. If possible let us assume that none among P and Q is normal in G. Then from Sylow's theorems n_5 divides 6 as $n_5 \equiv 1 \mod 5$, the possibilities are $n_5 = 1, 6$. Since $Q \not\trianglelefteq G$ it follows that $n_5 \neq 1$, therefore $n_5 = 6$. Similarly n_3 divides 10 and $n_3 \equiv 1 \mod 3$ which gives $n_3 = 10$. The total number of distinct-elements of G contained in these groups is equal to $10 \times 2 + 6 \times 4 + 1 = 45 > 30$ a contradiction as total number of elements in G is 30. Thus either $P \trianglelefteq G$ or $Q \trianglelefteq G$. Therefore $PQ = QP$ and $PQ \leq G$. Since $P \cap Q = 1$, it follows that $|PQ| = |P||Q| = 15$. Thus $[G : PQ] = 2$ therefore $PQ \trianglelefteq G$.

Example: (Groups of order $p^2q,\ p \neq q$). Let G be a group of order p^2q where p and q are distinct primes. If $q < p$ Then n_p divides q. Since $1 < q < p$ and $n_p \equiv 1 \mod p$, it follows that $n_p = 1$. In this case Sylow$-p-$subgroup of G is normal in G and G is not simple.
If $p < q$ then n_q divides p^2 and $n_q \equiv 1 \mod q$. Therefore choices are $n_q = 1, p, p^2$. If $n_q = 1$ then again G is not simple. Since $p < q$, $n_p \neq 1$. If $n_q = p^2$, then n_q divides $p^2 - 1 = (p - 1)(p + 1)$, since $p - 1 < q$ and q is a primes q does not divide $p - 1$, therefore q divides $p + 1$ which is possible if and only if $p = 2$ and $q = 3$. In this case $|G| = 2^2 \times 3 = 12$. If $n_3 \neq 1$ then $n_3 = 4$ and we will show later on using Cayley's theorem that here $G \cong A_4$.

Example: (Groups of order 99). Let $|G| = 99 = 3^2\times11$. Clearly here $n_3 = 1 = n_{11}$, therefore G is not simple. Let P be sylow$-3-$subgroup and Q is Sylow$-11-$subgroup of G. It follows that $PQ \leq G$. Since $P\cap Q = \{1\}$, $|PQ| = |P||Q| = 9 \times 11 = 99 = |G|$, hence $PQ = G$. We prove that G is abelian. First note that P and Q are abelian. If $x \in P$ and $y \in Q$, consider the element $xyx^{-1}y^{-1} \in G$. We have $P \ni \underbrace{x}_{\in P}\underbrace{yx^{-1}y^{-1}}_{\in P\cdot\because P\trianglelefteq G} = \underbrace{xyx^{-1}}_{\in Q\cdot\because Q\trianglelefteq G}\underbrace{y^{-1}}_{\in Q} \in Q$. It follows that $xyx^{-1}y^{-1} \in (P \cap Q) = \{1\}$, therefore $xyx^{-1}y^{-1} = 1$ or $xy = yx$. Therefore $PQ = G \cong Z_{99}$ or $Z_3 \times Z_{33}$.

Example: (Simple Group of order 60). Let $|G| = 60$ such that G has more than one Sylow$-5-$subgroup i.e. $n_5 > 1$. We show that G must be simple. To the contrary let if possible $H \trianglelefteq G$ where $H \neq 1, G$. Since n_5 divides 12 and $n_5 > 1$ therefore $n_5 = 6 \equiv 1 \mod 5$. Then $|N_G(H)| = 10$. If 5 divides $|H|$ then H contains a Sylow$-5-$subgroup of G. Since $H \trianglelefteq G$ it contains all conjugates of the Sylow$-5-$subgroups. Therefore $|H| \geq 6 \times 4 + 1 = 25$ and as $|H|$ divides 60. It follows that $|H| = 30$. This is a contradiction since from an earlier example 0.2 we have proved that any group of order 30 has unique Sylow$-5-$subgroup. Therefore 5 does not divide $|H|$. If $|H| = 6$ or 12 then H has normal Sylow subgroups which are therefore normal in G. Since we need to work with proper normal subgroup of G we may assume w.l.o.g. that $|H| = 2, 3, 4$. Let $\bar{G} = G/H$ then $|\bar{G}| = 30, 20, 15$. In each case G has a normal subgroup $\bar{H}$ of order 5. From 4th isomorphism theorem $\bar{P} = \frac{H_1}{H}$

for some $H_1 \trianglelefteq G,\ H_1 \neq G$. Then $|H_1| = |H||\bar{P}| = 5|H|$ this means 5 divides $|H_1|$ which is a contradiction, since it was assumed that 5 does not divide order of any of the proper normal subgroup of G. Therefore G is simple.

Example: (Groups of order 66). Let $|G| = 66 = 2 \times 3 \times 11$. Then clearly $n_{11} = 1$. Let P be a Sylow$-3-$subgroup and Q be the Sylow$-11-$subgroup of G. As $Q \trianglelefteq G$, it follows that $PQ \leq G$. Since $[G : PQ] = 2$, $PQ \trianglelefteq G$. Also note that as $|PQ| = 33 = 3 \times 11$, and 3 does not divide $11 - 1 = 10$, PQ is cyclic. Let $PQ = \langle x \rangle$. Let y be an element of G of order 2. Since $PQ \trianglelefteq G$ the conjugate $yxy^{-1} \in PQ$. Therefore there exists an $i \in \{1, 2, ..., 32\}$ such that $yxy^{-1} = x^i$ or $yx = x^i y$. First note that $|x^i| = |yxy^{-1}| = 33$ therefore $\gcd(i, 33) = 1$. Also $(yxy^{-1})^i = yx^i y^{-1} = x^{i^2}$ which gives

$$y(yxy^{-1})y^{-1} = x^{i^2}$$

or $x^{i^2-1} = 1$. Therefore 33 divides $(i-1)(i+1)$. The only values of i satisfying this condition are $i = 1, 32, 10, 23$. This proves that there are at most four groups of order 66. We have 4 non ismorphic groups of order 66 which are: $Z_{66}, D_{66},\ D_{22} \times Z_3$, and $D_6 \times Z_{11}$. Hence there are exactly four groups of order 66.

Example: (Group of order 255). Let $|G| = 255 = 3 \times 5 \times 17$. As n_{17} divides 15 and $n_{17} \equiv 1 \mod 17$, it follows that $n_{17} = 1$. Denote the Sylow$-17-$subgroup of G by P s.t. $P \trianglelefteq G$ and $P = \langle x \rangle$. If $n_5 \neq 1$ and $n_3 \neq 1$ then $n_5 = 51$, and $n_3 = 85$ therefore total number of elements of G within 51 Sylow$-5-$subgroups and 85 Sylow$-3-$subgroups is $51 \times 4 + 85 \times 2 + 1 = 375 > 255$ which is absurd. So either $n_5 = 1$ or $n_3 = 1$. Let $n_5 = 1$ and denote the Sylow$-5-$subgroup by Q. Take a Sylow$-3-$subgroup R. Observe that $[G : N_G(R)] = 85$ therefore $|N_G(R)| = 255/85 = 3$. Since $R \leq N_G(R)$ and $|R| = 3$, it follows that $N_G(R) = R$. Let $R = \langle y \rangle$. Then $|y| = 3$ and every element of order 3 in G is in R. Now for all $g \in G$, $|gyg^{-1}| = |y| = 3$, this shows that $gyg^{-1} \in R$ or $gRg^{-1} = R$ i.e. $n_3 = 1$ a contradiction since n_3 was assumed to be equal to 85. Thus our supposition is wrong and $n_3 = 1$, i.e. $R \trianglelefteq G$. Since all the three Sylow-subgroup of G are normal, it follows that $PQ \trianglelefteq G$, and as $PQ \cap R = \{1\} = P \cap Q$, $|(PQ)R| = |PQ||R| = 255 = |G|$ we see that $(PQ)R = G$. Since $|PQ| = 85$ and every group of order 85 is cyclic it follows that PQ is cyclic. Let $PQ = \langle x \rangle$. Consider the element $R \ni \left(\underbrace{xyx^{-1}}_{\in R, \because R \trianglelefteq G} \underbrace{y^{-1}}_{\in R} \right) = \left(\underbrace{x}_{\in PQ} \underbrace{yx^{-1}y^{-1}}_{\in PQ, \because PQ \trianglelefteq G} \right) \in PQ$. It follows that $xyx^{-1}y^{-1} \in (PQ \cap R) = \{1\}$. Thus $xy = yx$. Since any element of PQR is of the form $x^a y^b$ for some integers a and b, it follows that $x^a y^b = y^b x^a$. This proves that G is abelian. Since $PQ \leq \langle xy \rangle$ and $R \leq \langle xy \rangle$ therefore $G = PQR \leq \langle xy \rangle$ this proves that $G = \langle xy \rangle$, this proves that G is cyclic. We have proved that every group of order 255 is cyclic.

Definition: A finite group whose order is a prime power is called a $p-$group.

Theorem 0.5. *Let G be a finite group. Then every $p-$group as a subgroup of G is contained in some Sylow$-p-$subgroup of G.*

Proof. Let P be a Sylow$-p-$subgroup of G and H be a subgroup of G whose order is a power of p. Consider the action of H on the set $X := \{xPx^{-1} \mid x \in G\}$ via conjugation i.e.

$$h \bullet (xPx^{-1}) = (gx)P(gx)^{-1}.$$

Under this action $|\mathcal{O}_{xPx^{-1}}||\mathrm{Stab}(xPx^{-1})| = |H|$ therefore $|\mathcal{O}_{xPx^{-1}}|$ is a power of p. Also $n_p = |X| = \sum_{x \in G} |\mathcal{O}_{xPx^{-1}}|$ is not divisible by p, therefore there is at least one $y \in G$ for which p does not divide $|\mathcal{O}_{yPy^{-1}}|$, the only possibility is

$$|\mathcal{O}_{yPy^{-1}}| = 1.$$

Then $H = \mathrm{Stab}(yHy^{-1}) := \{g \in H \mid g(yPy^{-1})g^{-1} = yPy^{-1})\} \leq N_H(yPy^{-1})$.
Claim. *if $z \in N_H(yPy^{-1})$ such that $|z| = p^j$ for some positive integer j, then $z \in yPy^{-1}$.*
Proof of claim. To prove the claim, note that

$$[G : N_G(yPy^{-1})][N_G(yPy^{-1}) : yPy^{-1}] = [G : yPy^{-1}]$$

which shows that p does not divide $[N_G(yPy^{-1}) : yPy^{-1}] \geq [N_H(yPy^{-1}) : yPy^{-1}]$. Thus p does not divide $[N_H(yPy^{-1}) : yPy^{-1}]$. Consider the quotient group $N_H(yPy^{-1})/(yPy^{-1}) \ni z(yPy^{-1})$, then

$$(z(yPy^{-1}))^{p^j} = z^{p^j}(yPy^{-1}) = (yPy^{-1})$$

which shows that $|z(yPy^{-1})|$ divides p^j and also $|z(yPy^{-1})|$ divides $[N_H(yPy^{-1}) : yPy^{-1}]$. The only possibility is $|z(yPy^{-1})| = 1$ i.e. $z \in (yPy^{-1})$. This proves the claim.
Now as $H \leq N_H(yPy^{-1})$, and since every element of H is of the order equal to a power of p, by the above claim, it follows that $H \subseteq yPy^{-1}$. □

0.3 Miscellaneous

Example: (Probability that two group elements commute). Let G be a finite nonabelian group. We calculate the probability that the two group elements commute. For this the sample space is $G \times G$. For any

$(x, y) \in G \times G$, we need to obtain the cardinality of the set $S := \{(x, y) \in G \times G \mid xy = yx\}$. Note that for any $(x, y) \in S$ $xy = yx$ if and only if $y \in \text{Stab}(x)$ under the action of G on itself via conjugation. Therefore $\text{Stab}(x) \subseteq S$ for all $x \in G$. Since $|\text{Stab}(x)| = |g\text{Stab}(x)|$ for all $x, g \in G$, it follows that $|S| = \sum_{x\in G} |\text{Stab}(x)| = \sum_{x\in G} \frac{|G|}{|\mathcal{O}_x|}$. It follows that small the number of elements in an orbit, bigger is the number of elements in S. The minimum size of an orbit of x is 1 which corresponds to $x \in Z(G)$ otherwise for $x \notin Z(G)$ the minimal size of any orbit of x is 2. Therefore We have

$$|S| \leq |G||Z(G)| + \frac{|G|}{2}(|G| - |Z(G)|)$$

$$= \frac{|G|}{2}(|G| + |Z(G)|)$$

it follows that required probability is always $\leq \frac{1}{2}\left(1 + \frac{|Z(G)|}{|G|}\right)$. Since G is non-abelian then $|G/Z(G)| \geq 4$ (because if $G/Z(G)$ is cyclic then G is abelian). Therefore we have the maximum probability that the two group elements in a nonabelian group commute is given by

$$\frac{1}{2}\left(1 + \frac{1}{4}\right) = \frac{5}{8}.$$

The following result is very useful in characterizing unique group of a given finite order.

Theorem 0.6. Gallian and Moulton(1993). *There is unique abelian group (upto isomorphism) of order n if and only if* $\gcd(n, \varphi(n)) = 1$.

Proof. $\Leftarrow$**(Q implies P)** Let $\gcd(n, \varphi(n)) = 1$ then n is square free i.e. $n = p_1 \cdots p_r$ where $p_1, ..., p_r$ are distinct primes. We use induction on number r of distinct primes in prime decomposition of n. If $r = 1$ $|G| = p_1$ and therefore G is cyclic of prime order p_1. Let the result is true for all groups of order $n = p_1 \cdots p_k$ for all $k \leq r - 1$ and $\gcd(n, \varphi(n)) = 1$. Now let $n = p_1 \cdots p_r$ such that $\gcd(n, \varphi(n)) = 1$. W.l.o.g. let p_r is the largest among all primes $p_1, ..., p_r$. Using Sylow's third theorem $n_{p_r} = 1$ and the Sylow$-p_r-$subgroup H of G is normal in G. Consider the quotient group G/H where $|G/H| = p_1 \cdots p_{r-1}$ such that $\gcd(p_1 \cdots p_{r-1}, \varphi(p_1 \cdots p_{r-1})) = 1$, by induction hypothesis G/H is cyclic. Therefore there is an element $z \in G$ such that $G/H = \langle zH \rangle$ and $(zH)^{p_1 \cdots p_{r-1}}H = H$. This gives $1 \neq z^{p_1 \cdots p_{r-1}} \in H$. Since H is cyclic of prime order p_r, it follows that $(z^{p_1 \cdots p_{r-1}})^{p_r} = 1$ or $z^{p_1 \cdots p_r} = 1$, which proves that $|z| = |G|$, i.e. G is cyclic. This completes the final step of induction.

$\Rightarrow$**(Not$Q$ implies Not$P$)** Conversely let $\gcd(n, \varphi(n)) \neq 1$. If n is not square free then there is a prime p such that p^2 divides n. Then the group $Z_p \times Z_{\frac{n}{p}}$ is not cyclic. So let n is square free. Then there are at least two distinct primes p and q dividing n such that $q < p$ and q divides $p - 1$ then $(\mathbb{Z}/p\mathbb{Z})\times$ is a cyclic group of order $p - 1$ which by Cauchy's theorem has an element $\bar{s}$ of order q since q is a divisor of $p - 1$. Then the group $H = \left\langle a, b \mid a^q = b^p = 1,\ a^{-1}ba = b^s \right\rangle$ is a non abelian group of order pq and $H \times Z_{\frac{n}{pq}}$ is a noncyclic group of order n. □

As a consequence of this theorem we see that for any prime p, $\gcd(p, \varphi(p)) = \gcd(p, p - 1) = 1$ therefore any group of a prime order p is unique i.e. it is $\mathbb{Z}_p$. We list unique groups of composite orders from $1 - 100$ in the following table.

$\lvert G\rvert$	$\varphi(n)$	$\gcd(n, \varphi(n))$
15	8	1
33	20	1
35	24	1
51	32	1
65	48	1
69	44	1
77	60	1
85	64	1
87	56	1
91	72	1
95	72	1

Yet another result provides an answer to the following question: "For which positive integer n every group of order n is abelian?"

Theorem 0.7. Dickson(1905). *Every group G of order n is abelian if and only if n is of the form*

$$n = p_1 \cdots p_r q_1^2 \cdots q_s^2,$$

$$\gcd(n, (p_1 - 1) \cdots (p_r - 1)(q_1^2 - 1) \cdots (q_s^2 - 1)) = 1,$$

for some positive integers r and s where p_i and q_j are distinct primes.

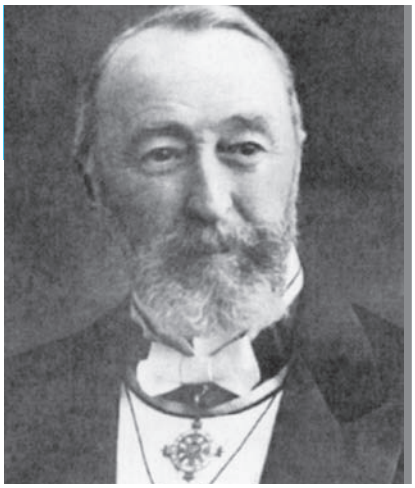
From the Dickson's theorem following can be deduced at once

- Every group of order p^2 is abelian since $n = p^2$ and $\gcd(p^2, p^2 - 1) = 1$.
- Also if we consider a group G such that $|G| = pq^2$ for some distinct primes p and q then G is abelian if and only if $\gcd(pq^2, (p - 1)(q^2 - 1)) = 1$.
- If $|G| = pqr$ where $p < q < r$ are distinct primes such that $\gcd(pqr, (p-1)(q-1)(r-1)) = 1$ then G is abelian, infact G is cyclic as well. In particular every group of order $105 = 3 \cdot 5 \cdot 17 = 255$ is cyclic!

Let us make a table for such groups ranging with composite orders from 2 to 100 by denoting

$$K := \prod_i (p_i - 1) \prod_j (q_j^2 - 1)).$$

$\lvert G\rvert$	Form of n	K	$\gcd(n, K)$
4	q^2	3	1
9	q^2	8	1
15	pq	8	1
25	q^2	24	1
33	pq	20	1
35	pq	24	1
45	pq^2	32	1
49	q^2	48	1
51	pq	32	1
65	pq	48	1
69	pq	44	1
77	pq	60	1
85	pq	64	1
87	pq	56	1
91	pq	72	1
95	pq	72	1
99	pq^2	80	1



Ludwig Sylow (pronounced 'see-low') was a Norwegian Mathematician born on December 12, 1832, in Christiania, Norway. He worked as a a high school teacher in 1855. Despite the long time required by his teaching duties, Sylow found time to study the work of Abel. During 18621863, Sylow got a temporary appointment at Christiania University and gave lectures on Galois theory and permutation groups. From 1873 to 1881, Sylow, with some help from his student Lie, prepared a new edition of Abels works. In 1902, Sylow and Elling Holst published Abels correspondence. **Sylows great discovery, Sylows Theorem, came in 1872**. Upon learning Sylows result, C. Jordan called it 'one of the essential points in the theory of permutations.' The result took on greater importance when the theory of abstract groups flowered in the late 19th century and early 20th century. In 1869, Sylow was offered a professorship at Christiania University but turned it down. Upon Sylows retirement from high school teaching at age 65, Lie mounted a successful campaign to establish a chair for Sylow at Christiania University. Sylow held this position until his death on September 7, 1918. For more about Sylow, visit: `http://www-groups.dcs.st-and.ac.uk/~history`

References:

[1] D.S. Dummit and R.M. Foote. *Abstract Algebra*, John Wiley (2007).

[2] Surjeet Singh and Q. Zameeruddin, *Modern Algebra*, Vikas Pub. Eighth Ed. (2009).

[3]* Joseph A. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole Pub. 7th Ed. (2010).

[4] Book by Gallian is an excellent text in abstract algebra which is full of motivation, applications, and historical development of the subject. Therefore this book is strongly recommended.

[5] Joseph A. Gallian and D. Moulton. When is Z_n the only Group of order n? *El. Math.* **48**, (1993) 117-119.

[6] L.E. Dickson. Definition of a group and a field by independent postulates. *Trans. Amer. Math. Soc.*, **6**, (1905) 198-204.

Exercises

1. Find all Sylow-3-subgroups of A_4.
2. Show that every group of order 56 has a proper nontrivial normal subgroup.
3. What is the smallest composite integer n such that there is a unique group of order n.
4. Let G be a noncyclic group of order 21. How many Sylow-3-subgroups does G have? How many elements of order 3 are there in G?
5. Prove that a group of order 175 is abelian.
6. What is a smallest possible odd integer that can be the order of a non-abelian group?
7. Suppose $|G| = p^n m$ where p is a prime such that

$p > m$. Prove that that $n_p = 1$.

8. Let $|G| = p^2q^2$ where p and q are distinct primes such that $q \nmid (p^2 - 1)$ and $p \nmid (q^2 - 1)$. Show that G is abelian. List three pairs of primes satisfying these conditions.

9. Establish the following results regarding $p-$groups:

   Let $|G| = p^n$ where p is a prime.

   (a) G has a normal subgroup of order p.

   (b) Show that G has normal subgroups of order p^k for all $k = 1, 2, ..., n$.[**Hint**: Use induction on n and the fact that $|Z(G)| \geq p$.]

   (c) If G has exactly one subgroup for each divisor of p^n, prove that G is cyclic.

   (d) If H is a proper subgroup of G, prove that $|N_G(H)| > |H|$. [**Hint**: Use Induction on n as in (b).]

10. For each prime p, prove that all Sylow$-p-$subgroups of a finite group G are isomorphic.

11. let p, q, r be distinct primes and $|G| = pqr$. Show that G is not simple.

12. Show that a group of order 225 is abelian.