Basic Group Theory

Nripendra Kumar Deb

November 2022

Definition:
Normaliser of a subgroup H of a group G is defined as

$$N(H) = \{g \in G \mid gHg^{-1} = H\}$$

Definition 2 :
Consider S to be the set of all conjugates of H. Consider the *stabilizer* of H under the conjugation action of G :

$$\text{stab}(H) = \{g \in G \mid gHg^{-1} = H\}$$

So $N(H) = \text{stab}(H)$ under the conjugation action of G on S.
• Further note that $H \subset N(H)$ and H is normal in $N(H)$, hence the name *normalizer*.
Remark: Both definitions have useful applications.

Lemma 1 :
If G be a group such that $|G| = p^k m$, and let S be the set of all $p-sylow$ subgroups with $P \in S$ be fixed then

$$|S| = [G : N(P)]$$

Proof : Firstly, recall that any two $p-sylow$ subgroups of a group G are conjugates of each other and any conjugate of a $p-sylow$ is agin a $p-sylow$(as conjugates have same cardinality). Thus S is in fact the set of all conjugates of P. Consider the conjugation action of G on S. Consider any two $p-sylow$ subgroups P_1 and P_2 of G. Since P_1 and P_2 are conjugates of each other so $\exists g \in G$ s.t $gP_1g^{-1} = P_2$ or $g.P_1 = P_2$[1] , which proves the *transitivity* of the action.

[1]Here $'g.'$ represents the action

Let $P \in \mathcal{O}$ where $\mathcal{O}$ is an orbit, since the action is *transitive* $\mathcal{O} = S$. From the orbit stabilizer theorem we have $|\mathcal{O}| = \frac{|G|}{|G_p|}$ i.e

$$|\mathcal{O}| = [G : G_P]$$

Here G_P is the *stabilizer* of P. Now using definition 2 we get $G_P = N(P)$ which gives

$$|\mathcal{O}| = |S| = [G : N(P)]$$

Lemma 2 :
If $H_1 \subset H_2 \subset G$, then $[G : H_2]$ divides $[G : H_1]$.
Proof : Let $[G : H_1] = m$ and $[G : H_2] = n$. Using counting formulae we have

$$|G| = m|H_1|$$

$$|G| = n|H_2|$$

using these we get

$$\frac{|H_2|}{|H_1|} = \frac{m}{n}$$

Lagrange Theorem tells that $|H_1|$ divides $|H_2|$ and hence n divides m.
Theorem 1 :
If G be a group such that $|G| = p^k m$, and let S be the set of all $p-sylow$ groups then $|S|$ divides m.

Proof : Fix one $P \in S$. Using *Lemma 1* we have

$$|S| = [G : N(P)]$$

Note that $P \subset N(P)$ and $[G : P] = m$ hence invoking *lemma 2* we get $|S|$ divides m.
Lemma 3 : Let G be a $p-group$ such that G acts on X and X^G is the set of all fixed points of X, then

$$|X^G| \equiv |X| \pmod p$$

Corollary: If p does not divide $|X|$, then X has a fixed point.
Proof : Using *lemma 3* we have

$$|X^G| \equiv |X| \pmod p$$

i.e p divides $|X^G| - |X|$ and as p does not divide $|X|$ so p must not divide $|X^G|$(why?). Since P does not divide $|X^G|$ hence $|X^G| > 0$ or X^G is non-empty, we are done.
Theorem 2 :
If G be a group such that $|G| = p^k m$, and let S be the set of all $p-sylow$ groups then

$$|S| \equiv 1 \pmod p$$

Proof : Note that setting $X = S$ as in *lemma 3* leaves us to show that S has a unique fixed point or $|X^G| = 1$. One can easily notice that $P \in S$ is a $p-group$. So we take action of P on the set S via conjugation. Let Q be a fixed point in S then $gQg^{-1} = Q$ for all $g \in P$ which implies $P \subset N(Q)$. Now note that Q is normal in $N(Q)$ and so Q is a unique $p-sylow$ in $N(Q)$ but P is also a $p-sylow$ in $N(Q)$[2] thus $P = Q$, which proves that the fixed point is unique. Hence we get

$$|S| \equiv 1 \pmod p$$

Exercise Let N be a nontrivial normal subgroup of a p-group G. Show that N must intersect the center of G non trivially.
Solution :
Let's take the conjugation action of G on N . The action is justified because the subgroup N is normal. Using Class equation we have:

$$|N| = |Z_N(G)| + \sum_{|\mathcal{O}_i|>1} |\mathcal{O}_i|$$

Here $Z_N(G)$ consists of the single orbits i.e let $\{x\} \in Z_N(G)$ then $x \in N$ and $gxg^{-1} = x \; \forall g \in G$. In fact note that if $Z(G)$ is the center of the group then

$$N \cap Z(G) = Z_N(G)$$

Note that p divides $|Z_N(G)|$ so

$$|N \cap Z(G)| = |Z_N(G)| > 0.$$

Exercise Let G be a p-group and let p^k be a divisor of $|G|$. Show that G has a subgroup of order p^k.
Solution :
Let's assume $|G| = n$ we will do induction on n. For $n = 1$, G is a cyclic group, so there exists elements of order 1 and p. Hence base case holds. Suppose that it holds for $|G| \in \{1, ..., p^{n-1}\}$. Consider a group G such that $|G| = p^n$. Since G is a p-group so C is non-trivial. Let $|C| = p^l$ now consider the group G/C(Why is this a group?). Then $|G/C| = p^{n-l}$, by induction hypothesis there exist a subgroup H/C ($H \subset G$) such that $|H/C| = p^{k-l}$ as $k \le n \Rightarrow k - l \le n - l$. So

$$|H| = |C| \times p^{k-l} \Rightarrow |H| = p^k.$$

Exercise There are 6 subsets of order 2 of $\{1, 2, 3, 4\}$. Any element of S_4 permutes these subsets.Show that the resulting homomorphism from S_4 to S_6 is injective and its image lies

[2] Since P and Q both belong to S so $|P| = |Q|$

in A_6.

Solution :

Let $\sigma \in S_4$ and we define $f : S_4 \mapsto S_6, f(\sigma)((i,j)) = (\sigma(i), \sigma(j))$.

$$f(\sigma_1\sigma_2)((i,j)) = (\sigma_1\sigma_2(i), \sigma_1\sigma_2(j)) = f(\sigma_1)((\sigma_2(i), \sigma_2(j))) = f(\sigma_1)f(\sigma_2)((i,j))$$

$$\Rightarrow f(\sigma_1\sigma_2) = f(\sigma_1)f(\sigma_2)$$

Hence f is a homomorphism. Let $f(\sigma_1) = f(\sigma_2)$ then $\sigma_1 = \sigma$ follows directly (Check!!). So f is injective. Note that if σ_1 and σ_2 both belong to same conjugacy class then $\sigma_1 = \sigma\sigma_2\sigma^{-1}$ then $f(\sigma_1) = f(\sigma_2)$. So we have to check the image for one element per conjugacy class. Note that a conjugacy class consists of elements one same cycle type exactly. Check that the images lies in A_3.

Exercise Show that there are 36 Sylow 5-subgroups in A_6.

Solution :

Note that $|A_6| = 120 = 2^2.3^2.5$. And order of $5-$sylow subgroup is 5 so it is a cyclic group note that each 5-sylow contains 4 elements of order 4 so if total number of 5-sylow subgroups is m . Then total number order 5 elements is A_6 is $4m$ as other only 5-sylow subgroups contributes to order 5 elements. Order 5 element in A_6 is of cycle type $5^1 1^1$ which is same as numbers of elements of cycle type $5^1 1^1$, hence

$$4m = \frac{6!}{5^1 1^1.1!.1!} \Rightarrow 4m = 144 \Rightarrow m = 36.$$

Exercise Partition $\{1, ..., 6\}$ into two subsets S and T of order 3. Let P be the set of elements in A_6 which permute S and T either trivially or by a 3-cycle.

a) Show that $|P| = 9$ and P is a 3-Sylow subgroup.

b) Prove that each 3-Sylow subgroup of A_6 is of the above form.

c) Deduce that there are 10 3-Sylow subgroups of A_6.

Solution :

(a) Let $\{a, b, c\}$ and $\{d, e, f\}$ be two such subsets. Note that (abc),(acb) are the only possible 3-cycles of P which permute $\{a, b, c\}$ so there are 3 elements in P which permutes $\{a, b, c\}$ and similarly for $\{d, e, f\}$. So in total we have $3 \times 3 = 9$ elements. (Here it is assumed that the action of A_6 is taken on the whole set which in fact gives a permutation of the subsets). Since $A_6 = 2^2.3^2.5$ hence P is a 3-sylow subgroup.

(b) Since two p-sylows are conjugates of each other. So any 3-sylow subgroup will be a conjugate of the above subgroup and as conjugates have same cycle type so every element of any other 3-sylow will have same cycle type as that of the elements of the above subgroup and hence of that form.

(c) Since every 3-sylow subgroup is of the above form so the number of 3-sylow subgroups are basically the number of ways to select the two subsets. Note that the order of selecting the subsets doesn't matter. So total number of 3-sylow subgroups is $\frac{\binom{6}{3}}{2!} = 10$.

Exercise Show that there are $(p-2)!$ Sylow p-subgroups of S_p(p is a prime). Deduce that:

$$(p-1)! \equiv -1 \pmod p$$

Solution :

We have $|S_p| = p! = p(p-1)!$ so p-sylow subgroups of S_p has order p as its maximum power of p dividing $|S_p|$. So every p-sylow subgroup has $(p-1)$ elements of order p as they are cyclic. So total $n_p(p-1)$ order p elements are there.

Again elements of order p in S_p are precisely the p-cycles and number of p-cycles in S_p is $\frac{p!}{p} = (p-1)!$. Hence we get

$$n_p(p-1) = (p-1)! \Rightarrow n_p = (p-2)!$$

Now using sylow's theorem and a bit of modular arithmetic we get

$$\begin{aligned}
&n_p \equiv 1 \pmod p \\
\Rightarrow\ &(p-2)! \equiv 1 \pmod p \\
\Rightarrow\ &(p-1)(p-2)! \equiv (p-1) \pmod p \\
\Rightarrow\ &(p-1)! \equiv -1 \pmod p
\end{aligned}$$

Exercise Let H be a subgroup of a G. If H is a p-group, show that H is contained in a p-Sylow subgroup of G.

Solution :

Consider a p-sylow subgroup P and the set G/P. Act H on this set via left multiplication. Note that if X is a set and a p-group acts on X then if p does not divide $|X|$ then X has a fixed point[3]. So here G/P has a fixed point gP say. Then $\forall\, h \in H$ we have

$$hgP = gP \Rightarrow g^{-1}hgP = P \Rightarrow g^{-1}hg \in P \Rightarrow h \in gPg^{-1}$$

Thus we get $H \subset gPg^{-1} = P'$, note that P' is also a p-sylow subgroup as cardinality of conjugate subgroups are equal.

Exercise Let H be a subgroup of G and let P be a p-Sylow subgroup of G.

a) Show that $H \cap P'$ is a p-Sylow subgroup of H where P' is a conjugate of P.

b) Show that G can be embedded in $GL_n(\mathbb{F}_p)$ for suitable n.

Solution :

(a) Consider the similar set and action as the previous question. Since p does not divide $|G/P|$ so by class equation we know there exists some orbit $\mathcal{O}$ of H such that p does not divide $|\mathcal{O}|$ and so $|\mathcal{O}| = 1$. Let $gP \in \mathcal{O}$ then by Orbit stabilizer theorem we get

$$|H| = |stab(gP)||\mathcal{O}|$$

[3] Use $|X| \equiv |X^G| \pmod p$

Note that

$$\begin{aligned} stab(gP) &= \{h \in H \mid hgP = gP\} \\ &= \{h \in H \mid g^{-1}hgP = H\} \\ &= \{h \in H \mid g^{-1}hg \in P\} \\ &= \{h \in H \mid h \in gPg^{-1}\} = \{h \mid h \in (H \cap gPg^{-1})\} \end{aligned}$$

Hence we get $stab(gP) = H \cap P'$, here $P' = gPg^{-1}$ and since $H \cap P' \subset P'$ so $|H \cap P'|$ divides $|P'|$ and thus $|H \cap P'| = p^m$ again p does not divide $|\mathcal{O}|$ so $H \cap P'$ is a p-sylow in H.

(b) **Just an Attempt**

If $|G| = n$ then using Cayley's Theorem we know that G can be embedded in S_n. Let $\beta = \{\epsilon_1, ..., \epsilon_n\}$ be the standard basis of $\mathbb{R}^n$. And for $\sigma \in S_n$ let $T_\sigma(\epsilon_i) = \sigma(\epsilon_i)$ here σ permutes β , P_σ be matrix representation of T_σ. Now consider the map

$$f : S_n \to GL_n(\mathbb{F}_p), \qquad \sigma \mapsto P_\sigma$$

Note that this map f is an isomorphism, so s_n can be embedded in $GL_n(\mathbb{F}_p)$. Hence indeed G can be embedded in $GL_n(\mathbb{F}_p)$.

(c) Note that $GL_n(\mathbb{F}_p)$ has a $p-$sylow subgroup consisting of upper triangular matrices with diagonal entries 1. Let P be one such p-sylow subgroup, and $Im(G)$ is the image of G embedded in $GL_n(\mathbb{F}_p)$ then using part (a) $P' \cap Im(G)$ has a p-sylow subgroup in $Im(G)$,taking the pre-image of that subgroup gives a p-sylow subgroup of G.

Exercise Let N be a normal subgroup of G. If P is a Sylow subgroup of G, show that $N \cap P$ is a Sylow subgroup of N.

Solution :

Using previous exercise we know that there exists some P' such that $N \cap P'$ is a p-sylow subgroup in N. We claim that $N \cap P = N \cap P'$. It follows

$$N \cap P' = N \cap gPg^{-1} = gNg^{-1} \cap gPg^{-1} \overset{?!}{=} g(N \cap P)g^{-1}$$

Note that conjugate of sylow group is a sylow group(check cardinality). Hence $N \cap P$ is a p-sylow subgroup of N.

Exercise let $f : G \to G'$ be a surjective homomorphism. If P is a sylow subgroup of G then $f(P)$ is also a sylow subgroup of G'.

Solution :

Consider $G = p^k.m$ such that $gcd(p, m) = 1$ and $|P| = p^k$ so $[G : P] = m$. Since f is a sujective homomorphism so $Im(f) = G'$. Using First isomorphism theorem[4] we get

$$|G| = |ker(f)||G'|$$

[4]If $f : G \to G'$ is a homomorphism then $G/ker(f) \cong Im\ f$

If we restrict the domain of f to P we get

$$|P| = |ker(f) \cap P||f(p)|$$

We get

$$\frac{[G : P]}{[G' : f(P)]} = \frac{|G||f(P)|}{|G'||P|} = \frac{|ker\ f|}{|ker(f) \cap P|}$$

By Lagrange's theorem $|ker(f) \cap P|$ divides $|ker\ f|$ so $[G' : f(P)]$ divides $[G : P]$. Since $|f(P)|$ divides $|P|$ so $f(P)$ is a p-group now we claim that $gcd([G' : f(P)], p) = 1$.
Indeed $[G' : f(P)]$ is a factor of $[G : P]$ and $[G : P], p$ are co-prime to each other so $[G' : f(P)]$ and p are also co-prime, which proves the fact that $f(P)$ is a sylow subgroup of G'.

Exercise Let H, H' be two subgroups of G such that H' normalizes H (i.e., H' is contained in $N(H)$). Show that HH' is a subgroup of G.

Solution :

We will use one step subgroup test here. Let h_1h_1' and h_2h_2' be two elements in HH'. Now

$$\begin{aligned} h_1{h_1}'(h_2{h_2}')^{-1} &= h_1{h_1}'({h_2}')^{-1}h_2^{-1} \\ &= h_1{h_1}'({h_2}')^{-1}h_2^{-1}{h_2}'({h_2}')^{-1} \\ &= h_1{h_1}'h({h_2}')^{-1} \\ &= h_1{h_1}'h({h_1}')^{-1}{h_1}'({h_2}')^{-1} \\ &= h_1h_0{h_1}'({h_2}')^{-1} \\ &= h_1h_0{h_3}' \end{aligned}$$

here $h = ({h_2}')^{-1}h_2^{-1}{h_2}' \in H$ as H' normalizes H. So $h_3' \in H'$ and $h_1{h_1}'(h_2{h_2}')^{-1} = h_1h_0h_3' \in HH'$.

Exercise Let N be the normalizer of a Sylow p- subgroup P of S_p. Show that $|N| = p(p-1)$.

Solution :

Let the S be the set of all p-sylows of S_p then using the definition 2 of normalizer and the proof of **lemma 1** we get

$$|S| = [S_p : N]$$

Now in one of the previous exercise we determined $|S| = (p-2)!$, hence it follows that

$$(p-2)! = \frac{|S_p|}{|N|} \Rightarrow |N| = \frac{p!}{(p-2)!} = p(p-1)$$