Chapter 24 Sylow Theorems

Conjugacy class

Definition Two elements $a, b \in G$ are conjugate in G if $b = x^{-1}ax$ for some $x \in G$. It is an equivalence relation with equivalence class $cl(a) = \{x^{-1}ax : x \in G\}$, known as the conjugacy class.

Example S_4, A_4, D_4.

Denote by $C(a) = \{x \in G : ax = xa\}$ the centralizer of $a \in G$.

Theorem 24.1 Let G be a finite group, and $a \in G$. Then

$$|cl(a)| = |G : C(a)| = |G|/|C(a)|.$$

Consequently, $|cl(a)|$ is a factor of $|G|$.

Proof. Define $T : \{xC(a) : x \in G\} \to cl(a)$ by $T(xC(a)) = xax^{-1}$. It is a well defined bijection. □

Corollary For any finite group G, $|G| = \sum |G : C(a)|$, where the sum runs through different representatives of the conjugacy relation.

Theorem 24.2 Let G be a p group, i.e., $|G| = p^m$ for some positive integer m. Then $|Z(G)| > 1$.

Proof. Suppose $|Z(G)| = 1$. Then

$$|G| = \sum |G : C(a)| = 1 + \sum_{a \neq 1} |G : C(a)|.$$

Corollary Let p be a prime number. A group with p^2 element is Abelian.

Proof. ...

Probability of choosing a commuting pair

Corollary Let G be a finite group with m conjugacy classes. The probability of choosing a commuting pair of elements from G at random is: m/n.

Proof. Consider $K = \{(x, y) : xy = yx\}$. Then $(x, y) \in K$ if and only if $y \in cl(x)$. Fix $a \in G$ with $cl(a) = \{a_1, \ldots, a_t\}$, where $t = |G|/|C(a)|$, and the number of (x, y) pairs in K equals

$$|C(a_1)| + \cdots + |C(a_t)| = t|C(a)| = |G|.$$

Thus, if there are m conjugacy classes, then $K = \sum_{x \in G} |C(x)| = m \cdot n$. The result follows. $\square$

Theorem 24.3/4 Let G be a finite group with order $p^\ell m$, where $p \not| m$.

1. G contains a subgroup of order p^k for each $k = 1, \ldots, \ell$.
2. Every subgroup H of G of order p^k is a normal subgroup of a subgroup of order p^{k+1} for each $k = 1, \ldots, \ell - 1$.

Proof. By induction on $|G|$. If $|G| = 1$, the result holds trivially. Suppose the result holds for groups of order at most $|G| - 1$. If G has a subgroup H of order $p^\ell r$ with $r < m$, then the result holds by induction. Assume that G has no such subgroup. Note that

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} |G : C(a)|.$$

Now, $p^k | n$ and $p^k \not| C(a)$. So, p is a factor of $|G|/|C(a)|$ for any $a \notin Z(G)$.

Hence, p is a factor of $Z(G)$, and $Z(G)$ has a subgroup N of order p.

If $\ell = 1$, we get the desired contradiction, namely, G has a subgroup of order p^ℓ. If not, by induction assumption on G/N, there is a sequence of subgroups $\tilde{H}_1 \leq \cdots \leq \tilde{H}_{\ell-1}$ of order $p, p^2, \ldots, p^{\ell-1}$ so that $\tilde{H}_i$ is normal in $\tilde{H}_{i+1}$ for $i = 1, \ldots, \ell - 2$.

Let $\phi : G \to G/N$ be the natural epimorphism $\phi(g) = gN$. Then $H_i = \phi^{-1}[\tilde{H}_i] \leq G$ will have order p^{i+1}, and the chain of subgroups $N \leq H_1 \leq \cdots \leq H_{\ell-1}$ in G such that $H_{\ell-1}$ is a subgroup of G with p^ℓ element, which is a contradiction.

Definition Let G be a finite group of order $n = p^\ell m$, where p is a prime and $p \not| m$. If $H \leq G$ such that $|H| = p^\ell$, then H is a Sylow p-subgroup of G.

Theorem 24.5(a) Any two Sylow p-subgroups of G are conjugate to each other.

Proof. Let $|G| = p^\ell m$ with $p \not| m$, and let K be a Sylow p-subgroup of G.
Suppose $C = \{K_1, \ldots, K_n\}$ is the set of conjugates of $K = K_1$. Then every K_j is a Sylow p-subgroup.
Suppose H is a Sylow p-subgroup of G. Consider the map $T : G \to S_C$ such that $g \mapsto \phi_g$, where

$$\phi_g(K_1, \ldots, K_n) = (gK_1g^{-1}, \ldots, gK_ng^{-1}).$$

Then T is a group homomorphism.
Now, $|H| = p^\ell$ so that the order of $T(H) = \{\phi_h : h \in H\}$ is a power of p because $T(H)/\mathrm{Ker}(\phi) \sim H$. Let

$$\mathrm{Orb}_{T(H)}(K_i) = \{hK_ih^{-1} : h \in H\}$$

$$\text{and} \qquad \mathrm{Stab}_{T(H)}(K_i) = \{h \in H : hK_ih^{-1} = K_i\}.$$

Then $|T(H)| = |\mathrm{Stab}_{T(H)}(K_i)||\mathrm{Orb}_{T(H)}(K_i)|$.

So, $|Orb_{T(H)}(K_i)|$ and $|Stab_{T(H)}(K_i)|$ are powers of p.

Homework 1 If $P < S_n$, then $|P| = |\mathrm{Stab}_P(i)||\mathrm{Orb}_P(i)|$.

Claim: There is i such that $|Orb_{T(H)}(K_i)| = 1$.

It will then follow that $hK_ih^{-1} = K_i$ so that $H < N(K_i)$, the normalizer of K_i, with order $p^\ell r$.

As a result, every $h \in H$ is an element of the Sylow p-subgroup of $N(K_i)$ so that $h \in K_i$. (**Homework 2.**)

To prove the claim, note that $|C| = |G : N(K)| = |G|/|N(K)|$.

Homework 3 If $H < G$, then the number of conjugates of H in G equals $|G : N(H)|$.

Now $|G|/|K| = (|G|/|N(K)|)(|N(K)/K|)$ so that $|C|$ is not divisible by p.

Observe that $|C| = \sum |\mathrm{Orb}_{T(H)}(K_i)| = \sum p^{r_i}$, which is not divisible by p.

Hence there is $r_i = 0$. $\square$

Theorem 24.5(b) Suppose G has order $p^\ell m$, where p is a prime and $p \nmid m$. Then the number n of Sylow p-subgroups of G satisfies $p|(n-1)$ and $n|m$.

Proof. Let K be a Sylow k-subgroup, and $C = \{K_1, \ldots, K_n\}$ be all its conjugate with $K = K_1$.

Claim 1. $n-1$ is divisible by p.

Consider $|\mathrm{Orb}_{T(K)}(K_i)| = p^{s_i}$ for each i, and $s_i = 0$ if and only if $K \leq K_i$. Thus, $s_1 = 0$ and $s_i > 0$ for all other i. The claim follows.

Claim 2. $|C| = n$ is a factor of m.

Note that $n = |C| = |G|/|N(K)| = p^\ell m/p^\ell t = m/t$. □

Corollary If G has only one Sylow p-subgroup H, then H is normal.

Theorem 24.6 Suppose $p < q$ are distinct primes such that p is not a factor of $q-1$. If $|G| = pq$, then G is cyclic.

Proof. By Theorem 25.5 (b), the number n_p of p-element group H has the form $1+kp$ and divides q and hence pq. So, $1+kp = 1, p, q, pq$. But p is not a factor of $q-1$. So, $k = 0$.

Similarly, there is only one subgroup K of order q.

If $H = \langle x \rangle$ and $K = \langle y \rangle$, then $xy = yx$ and $G = HK = \langle xy \rangle$.

There is only one subgroup of order p and one subgroup of order q, and G is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_q$. □

Examples

Example Sylow subgroups of S_3: 1 Sylow 3-subgroup; 3 Sylow 2-subgroup.

Example Sylow subgroups of A_4.

4 Sylow 3-subgroups, and 1 Sylow 2-subgroup containing 4 two element groups.

Example In D_{12}, there are seven subgroups of order 2. $\{R_0, R_{180}\}$ is not conjugate to the other 6 2-element subgroups.

Example A group of order 40. There is only one subgroup of order 5.

Reason. Suppose there are n such subgroups. Then $n = 1 + 5k$, and n is a factor of 8. So, $k = 0$.

There is/are 1 subgroup or 5 subgroups of order 8.

Reason. Suppose there are n such subgroups. Then $n = 1 + 2k$ and is a factor of 5 so that is is a factor of 5.

If the former holds, then $G = HK$.

If the latter holds, none of them is normal, and they are conjugate to each other.

More examples

Example A group of order 30.

There are 1 or 6 subgroup of order 5; 1 or 10 subgroup of order 3.

If there are 6 subgroups of order 5, and 10 subgroups of order 3, there will be more than 30 elements.

One of these subgroup is normal, and we can form $HK = \langle y \rangle$, a 15 element cyclic subgroup of G, which is normal in G so that $G/(HK) = \{HK, xHK\}$.

So, $G = \{x^i y^j : 0 \leq i \leq 1, 0 \leq j \leq 14\}$.

Example A group of 72 element has a non-trivial proper normal subgroup.

Reason: There are one or four 9-element subbroup.

If there is one, we are done. If not, let H_1, H_2 be two of such groups. Then $|H_1 H_2| = |H_1||H_2|/|H_1 \cap H_2| = 81/|H_1 \cap H_2|$ so that $|H_1 \cap H_2| = 3$.

Now, $|H_1| = |H_2| = 9$ so that H_1, H_2 are Abelian, and $H_1 \cup H_2 \subseteq N(H_1 \cap H_2)$. Moreover, $H_1 H_2 \subseteq N(H_1 \cap H_2)$ has at least $81/3 = 27$ elements. Since, $|N(H_1 \cap H_2)|$ divides 72, and divisible by 9. So, it is 36 or 72.

Example Suppose $|G| = 255 = 3 \cdot 5 \cdot 17$. Show that G is cyclic.

Proof. By the Sylow 17-subgroup H is normal so that $G = N(H)$.

Now, $|N(H)/C(H)|$ divides $|\mathrm{Aut}(H)| = |\mathrm{Aut}(\mathbb{Z}_{17})| = 16$ because $\phi : N(H) \to \mathrm{Aut}(H)$ defined by $\phi(g) = T_g : H \to H$ so that $T_g(x) = gxg^{-1}$ is a group homomorphism with kernel $C(H)$ so that $N(H)/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Because $|N(H)/C(H)|$ also divides 255. We conclude that $|N(H)/C(H)| = 1$. So, every $x \in N(H) = G$ lies in $C(H)$ implying x commutes with all elements in H.

Thus, $H \subseteq Z(G)$ and $|Z(G)| = 17, 51, 85, 255$ and $|G/Z(G)|$ is 15, 5, 3, 1.

So, $G/Z(G)$ is cyclic, and G is Abelian. Thus, G is cyclic.

Homework

1. Let $P < S_n$. Show that $|P| = |\mathrm{Stab}_P(i)||\mathrm{Orb}_P(i)|$.
   Hint: Prove that the map $\sigma\mathrm{Stab}_P(i) \mapsto \sigma(i)$ for $\sigma \in P$ is a bijection.
2. Let $H < G$ be such that $|H| = p^\ell$, $|G| = p^\ell m$, where $p \not| m$. Suppose $K_i < G$ with $|K_i| = p^\ell$, and $H < N(K_i) = \{g \in G : gK_ig^{-1} = K_i\}$.
   (a) Show that HK_i is a subgroup of $N(K_i)$ and
   $$|H||K_i|/|H \cap K_i| = |HK_i|.$$
   (b) Deduce that $|H \cap K_i| = |H|$ so that $H \subseteq K_i$.
3. Let $H < G$.
   (a) Show that $N(H) = \{g \in G : gHg^{-1} = H\}$ is a subgroup.
   (b) Show that the number of conjugates of H in G equals $|G : N(H)|$.