PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 12

INSTRUCTOR: ARUNDHATHI KRISHNAN

13. Sylow Theorems

13.1. Conjugacy classes.

Definition 13.1.1. Let G be a group and $a, b \in G$. We say that a and b are conjugate in G if $xax^{-1} = b$ for some $x \in G$. The conjugacy class of a is the set $\text{conj}(a) = \{xax^{-1} \mid x \in G\}$.

It is not hard to prove that conjugacy is an equivalence relation and thus the distinct conjugacy classes of elements of G form a partition of G.

Example 13.1.2. Let $G = D_4$. Then we get the following conjugacy classes: $\text{conj}(r_0) = \{r_0\}$, $\text{conj}(r_1) = \{r_1, r_3\} = \text{conj}(r_3)$, $\text{conj}(r_2) = \{r_2\}$, $\text{conj}(s_0) = \{s_0, s_2\} = \text{conj}(s_2)$ and $\text{conj}(s_1) = \{s_1, s_3\} = \text{conj}(s_3)$.

Theorem 13.1.3. *Let G be a finite group, $a \in G$ and $C(a) = \{x \in G \mid xa = ax\}$ be the centralizer of a. Then $|\,\text{conj}(a)\,| = |\,G : C(a)\,|$.*

Proof. Define the map T that sends the coset $xC(a)$ to the conjugate xax^{-1} of a. Now $xax^{-1} = yay^{-1}$ if and only if $x^{-1}ya = ax^{-1}y$ if and only if $x^{-1}y \in C(a)$, which in turn is true if and only if the cosets $xC(a)$ and $yC(a)$ are equal. Hence T is well-defined and one-to-one. It is clearly onto the conjugacy class of a. Hence the number of cosets of $C(a)$ in G given by the index $|\,G : C(a)\,|$ is equal to the number of conjugates of a, so that $|\,\text{conj}(a)\,| = |\,G : C(a)\,|$. □

Recall that we showed in Assignment 1 that $|\,G\,| = |\,\text{conj}(a\,|\,|\,C(a)\,|$ for each $a \in G$. This follows from Theorem 13.1.3 and the fact that for the finite group G, $|\,G : C(a)\,| = \frac{|\,G\,|}{|\,C(a)\,|}$. We get the following corollary immediately.

Corollary 13.1.4. *If G is a finite group, then $|\,\text{conj}(a)\,|$ divides $|\,G\,|$.*

Further, as distinct conjugacy classes form a partition of G, we also have the following consequence.

13.2. The class equation.

Corollary 13.2.1 (Class Equation)**.** *For any finite group G,*

$$|\,G\,| = \sum |\,G : C(a)\,|\,, \tag{1}$$

where the sum runs over one element from each conjugacy class of G.

The following theorem gives that a group of prime power order has a non-trivial centre.

Theorem 13.2.2. *Let G be a non-trivial finite group whose order is a power of a prime p. Then $Z(G)$ has more than one element.*

Proof. We observe that $\text{conj}(a) = \{a\}$ if and only if $gag^{-1} = a$ for each $g \in G$, which happens precisely if $a \in Z(G)$. Hence we can split the sum in (1) to get

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

The index $|\,G : C(a)\,| = \frac{|\,G\,|}{|\,C(a)\,|}$ for each a, hence each term in $\sum_{a\notin Z(G)} |\,G : C(a)\,|$ has the form p^k for $k \geq 1$. Hence $|\,G\,| - \sum_{a\notin G} |\,G : C(a)\,| = |\,Z(G)\,|$, so that p divides $|\,Z(G)\,|$ and $|\,Z(G)\,|$ cannot be 1.

□

This gives us a second proof of Theorem 9.4.1

Corollary 13.2.3. *If $|\,G\,| = p^2$, where p is a prime, then G is Abelian.*

Proof. By 13.2.2, $|\,Z(G)\,|$ is either p or p^2. If it is the latter, then $Z(G) = G$, so G is Abelian. On the other hand if it is the former, then $\left|{}^{G}\!/_{Z(G}\right| = p$, so ${}^{G}\!/_{Z(G)}$ is cyclic and hence by Theorem 9.3.2, G is Abelian. □

13.3. **The probability that two elements commute.** Before moving on to the Sylow theorems, consider this interesting problem. Given a finite group, how likely it is that two elements commute? If the group is Abelian, of course the probability is 1! Interestingly, we can use conjugacy classes to arrive at an answer in the general case. Namely, the larger the number of conjugacy classes, the larger the probability that two elements commute.

To find the probability that two elements of G commute we must compute:

$$p = \frac{|\,\{(x,y) \in G \times G \mid xy = yx\}\,|}{|\,G \times G\,|} = \frac{|\,K\,|}{n^2},$$

where $K = \{(x,y) \in G \times G \mid xy = yx\}$ and $n = |\,G\,|$.

Now $xy = yx$ if and only if $y \in C(x)$. Hence $|\,K\,| = \sum_{x\in G} |\,C(x)\,|$. If $z_1, z_2 \in \text{conj}(a)$ for some $a \in G$, then $\text{conj}(z_1) = \text{conj}(z_2)$, so that by Theorem 13.1.3, we also have $|\,C(z_1)\,| = |\,C(z_2)\,|$. Hence $\sum_{z\in\text{conj}(a)} |\,C(z)\,| = |\,\text{conj}(a)\,|\,|\,C(a)\,| = |\,G\,| = n$. Let m be the number of distinct conjugacy classes in G. Then $|\,K\,| = mn$, so that the probability $p = \frac{m}{n}$.

We get the maximum number of conjugacy classes if $|\,\text{conj}(a)\,| = 1$ for as many $a \in G$ as possible, which in turn is true if and only if $a \in Z(G)$, so for a higher probability, we want the center to be larger (this also fits in with our intuition!).

Now if G is not Abelian, then by Theorem 9.3.2, ${}^{G}\!/_{Z(G)}$ is not cyclic, hence it must have order greater than or equal to 4. Hence $|\,Z(G)\,| \leq \frac{|G|}{4}$. Hence if G is not Abelian, the maximum number of elements in $Z(G)$ is $\frac{|G|}{4}$. To get the maximum number of conjugacy classes, the remaining $\frac{3}{4}\,|\,G\,|$ elements must be in conjugacy classes of size 2. Hence the maximum number of conjugacy classes m is equal to $\frac{|G|}{4} + \frac{1}{2} \times \frac{3}{4}\,|\,G\,| = \frac{5}{8}\,|\,G\,| = \frac{5}{8}n$, and $p \leq \frac{m}{n} = \frac{5}{8}$. So in a non-Abelian group, the best possible probability that two elements commute is $\frac{5}{8}$. This upper bound is actually achieved in the group D_4 (check Example 13.1.2).

13.4. **Sylow Theorems.** Sylow's theorems tell us a great deal about a group just by using its order. The first theorem tells us that for any prime power that divides the order of a finite group, there exists a subgroup of that order. Hence we get a partial converse of Lagrange's theorem.

Theorem 13.4.1 (Sylow's first theorem)**.** *Let G be a finite group and p be a prime. If p^k divides G for some $k \in \mathbb{N}$, then G has at least one subgroup of order p^k.*

Proof. The proof is by induction on $|\,G\,|$. If G is trivial, then the theorem is trivially true as no prime power divides 1. Suppose the statement is true for all groups of order less than $|\,G\,|$.

The Class Equation (1) for G gives $|\,G\,| = |\,Z(G)\,| + \sum_{a \notin Z(G)} |\,G : C(a)\,|$. If p^k divides $|\,C(a)\,|$ for some $a \notin Z(G)$, then $C(a)$ is a proper subgroup of G such that p^k divides its order. So by the induction hypothesis, $C(a)$ has a subgroup of order p^k, and hence, so does G. We thus assume that for no $a \in Z(G)$ does p^k divides $|\,C(a)\,|$.

Hence we assume p^k divides $|\,G\,|$ but p^k does not divide $C(a)$ for each $a \notin Z(G)$ as $C(a)$ is a proper subgroup of G. As $|\,G\,| = |\,G : C(a)\,|\,|\,C(a)\,|$ and p is a prime, we must have that p divides $|\,G : C(a)\,|$ for each $a \notin Z(G)$. This gives in turn that p divides $Z(G)$. Now, $Z(G)$ is an Abelian group, hence by Cauchy's theorem (Theorem 9.3.4), $Z(G)$ contains an element of order p, say x. As $\langle x \rangle$ is a normal subgroup of G, $G/\langle x \rangle$ is a quotient group. Further, p^{k-1} divides $\left| G/\langle x \rangle \right|$, so by the induction hypothesis $G/\langle x \rangle$ has a subgroup of order p^{k-1}. It is left as an exercise to prove that this subgroup is of the form $H/\langle x \rangle$ where H is some subgroup of G (Hint: Use Theorem 10.2.2 (vii)).

Now $\left| H/\langle x \rangle \right| = p^{k-1}$ and $|\,\langle x \rangle\,| = p$, hence $|\,H\,| = p^k$ as required. □

Definition 13.4.2. Let G be of finite order and p be a prime. If p^k divides $|\,G\,|$ and p^{k+1} does not divide $|\,G\,|$, then any subgroup of order p^k is called a Sylow p-subgroup of G.

Suppose $|\,G\,| = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7$. Then Sylow's first theorem tells us that G has subgroups of orders $2, 4, 8, 3, 9, 5, 25, 125, 625$ and 7. Moreover, the Sylow 2-subgroup has order 8, the Sylow 3-subgroup has order 9, the Sylow 5-subgroup has order 625 and the Sylow 7-subgroup has order 7.

In other words, a Sylow p-subgroup of G is a subgroup whose order is the largest power of p consistent with Lagrange's theorem.

As every subgroup of prime order must be cyclic, we get the following corollary as a generalization of Theorem 9.3.4 (Cauchy's theorem).

Corollary 13.4.3. *Let G be a group of finite order and suppose p is a prime that divides $|\,G\,|$. Then G has an element of order p.*

Definition 13.4.4. Let H and K be subgroups of a group G. We say that H and K are conjugate in G if there exists $g \in G$ such that $H = gKg^{-1}$.

Recall that if $H = gKg^{-1}$, then H and K have the same order.

Lemma 13.4.5. *Let K be a Sylow p-subgroup of a finite group G. Recall that $N(K) = \{g \in G \mid gKg^{-1} = K\}$ is the normalizer of K. If $x \in N(K)$ and $|\,x\,|$ is a power of p, then $x \in K$.*

Proof. K is a normal subgroup of $N(K)$ and $\langle x \rangle$ a subgroup of $N(K)$ so that their product $\langle x \rangle K$ is a subgroup of $N(K)$. Suppose $|\,x\,| = p^l$ and $|\,K\,| = p^k$, then by Theorem 7.2.9,

$$|\,\langle x \rangle K\,| = \frac{|\,\langle x \rangle\,|\,|\,K\,|}{|\,\langle x \rangle \cap K\,|} = \frac{p^l p^k}{|\,\langle x \rangle \cap K\,|}.$$

Hence $|\,\langle x \rangle \cap K\,| \geq p^l$ as the subgroup $\langle x \rangle K$ is a subgroup whose order is a power of p, where the power cannot be greater than k. On the other hand $|\,\langle x \rangle \cap K\,| \leq p^l$, so that $\langle x \rangle \cap K = \langle x \rangle$ and $x \in K$. □

Here is a lemma analogous to Theorem 13.1.3.

Lemma 13.4.6. *Let K be a subgroup of a finite group G and let $C = \{K_1, \ldots, K_n\}$ be the set of conjugates of K. Then $|\, C \,| = |\, G : N(K) \,|$.*

Proof. Define the map T that sends the coset $gN(K)$ to the subgroup gKg^{-1}. As $gN(K) = hN(K)$ if and only if $h^{-1}g \in N(K)$, which in turn is true if and only if $h^{-1}gKg^{-1}h = K$, or $gKg^{-1} = hKh^{-1}$, the map T is well-defined and injective. It is is clearly onto C. Hence $|\, C \,|$ is given by the number of cosets of $N(K)$ in G, that is $|\, G : N(K) \,|$. □

Sylow's second theorem states that any subgroup of order some power of a prime p is contained in a Sylow p-subgroup of G.

Theorem 13.4.7 (Sylow's second theorem)**.** *If H is a subgroup of a finite group G and $|\, H \,|$ is a power of a prime p, then H is contained in some Sylow p-subgroup of G.*

Proof. Let K be a Sylow p-subgroup of G and let $C = \{K_1, \ldots, K_n\}$ with $K = K_1$ be the set of all conjugates of K in G. That is, $K_1 = eKe^{-1}$ and there exist $g_2, \ldots, g_n \in G$ such that $K_i = g_i K g_i^{-1}$. Each K_i is a Sylow p-subgroup of G.

Now $\varphi : G \times C \to C$ be given by $\varphi(g, K_i) = gK_ig^{-1}$ defines a group action and for $\varphi_g(K_i) := \varphi(g, K_i)$, the map $g \mapsto \varphi_g$ is a group homomorphism. By restricting the map $g \mapsto \varphi_G$ to H and applying the Orbit-Stabilizer theorem (Theorem 12.2.3) we have that $\left|\, \mathrm{orb}_H^{\varphi}(K_i) \,\right|$ divides $|\, H \,|$ and hence it is a power of p.

Now observe that $\left|\, \mathrm{orb}_H^{\varphi}(K_i) \,\right| = 1$ if and only if $gK_ig^{-1} = K$ for all $g \in H$, that is, if and only if $H \leq N(K_i)$. But as every element of H has order equal to some power of p, by Lemma 13.4.5, $\left|\, \mathrm{orb}_H^{\varphi}(K_i) \,\right| = 1$ if and only if $H \leq K_i$. Hence the theorem is proved if we prove that for some i, $\left|\, \mathrm{orb}_H^{\varphi}(K_i) \,\right| = 1$.

By Lemma 13.4.6, $|\, C \,| = |\, G : N(K) \,|$. As $|\, G : K \,| = |\, G : N(K) \,|\, |\, N(K) : K \,|$ and $|\, G : K \,|$ is not divisible by p, neither is $|\, G : N(K) \,| = |\, C \,|$. On the other hand, $|\, C \,|$ is equal to a sum of powers of p as the orbits partition C, hence at least one orbit must have size $p^0 = 1$, as required. □

Sylow's third theorem places some conditions on the number of Sylow p-subgroups of a group G.

Theorem 13.4.8 (Sylow's third theorem)**.** *Let p be a prime and G be a finite group with $|\, G \,| = p^k m$, where p does not divide m. Then with n denoting the number of Sylow p-subgroups of G, we have $n \equiv 1 \mod p$, and n divides m. Further, any two Sylow p-subgroups of G are conjugate.*

Proof. Let K be any Sylow p-subgroup of G and as before, let $C = \{K_1, \ldots, K_n\}$ be the set of conjugates of K with $K = K_1$. We will prove that $n \mod p \equiv 1$.

Recall the group action φ from Theorem 13.4.7 and the homomorphism $g \mapsto \varphi_g$. That is, $\varphi_g(K_i) = \varphi(g, K_i) = gK_ig^{-1}$ for each $g \in G$ and i. By the Orbit-Stabilizer theorem, $\left|\, \mathrm{orb}_K^{\varphi}(K_i) \,\right|$ divides $|\, K \,|$, so that it is a power of p for each i. Further, as observed in Theorem 13.4.7, $\left|\, \mathrm{orb}_K^{\varphi}(K_i) \,\right| = 1$ if and only if $K \leq K_i$. Thus $\left|\, \mathrm{orb}_K^{\varphi}(K_1) \,\right| = 1$ and $\left|\, \mathrm{orb}_K^{\varphi}(K_i) \,\right|$ is a power p^{l_i} for $l_i \geq 1$ for each $i \neq 1$. Since the orbits partition C, we get $n = |\, C \,| \equiv 1 \mod p$.

Next we show that every Sylow p-subgroup of G is in C. Suppose H is a Sylow p-subgroup of G that is not in C. Consider the group action φ restricted to $H \times C$. Then we know that $|\, C \,|$ is given by the sum of cardinalities of distinct orbits $\mathrm{orb}_H^{\varphi}(K_i)$ under the action of φ. No orbit has size 1 as H does not belong to C. Thus $|\, C \,|$ is a sum of terms divisible by p so $n \equiv 0 \mod p$. But this contradicts the fact that $n \equiv 1 \mod p$. Hence it must hold that

$H \in C$, and indeed that every Sylow p-subgroup is a conjugate of K, the Sylow p-subgroup with which we started.

Finally, $n = |C| = |G : N(K)| = \frac{|G|}{|N(K)|} = \frac{p^k m}{|N(K)|}$, so n divides $p^k m$. But as $\gcd(n, p) = 1$ (since $n \equiv 1 \mod p$), we must have that n divides m. □

Henceforth, we will denote the number of Sylow p-subgroups of a finite group G by n_p.

Corollary 13.4.9. *A Sylow p-subgroup of a finite group G is a normal subgroup if and only if it is the only Sylow p-subgroup of G.*

We will now apply the Sylow theorems to some familiar groups.

Example 13.4.10.

(i) Let $G = S_3$. Then $|G| = 3 \times 2$. Hence there exists a Sylow 2-subgroup. Further, n_2 divides 3 and $n_2 \equiv 1 \mod 2$. In fact, n_2 is equal to 3 as $K_1 = \{(1), (1, 2)\}, K_2 = \{(1), (2, 3)\}$ and $\{(1), (1, 3)\}$ are all subgroups of order 2. It is not hard to verify that $K_2 = (1, 2)K_1(1, 2)^{-1}$ and $K_3 = (2, 3)K_1(2, 3)^{-1}$.

(ii) Let $G = A_4$. Then $|G| = 12 = 3 \times 2^2$, so G has a Sylow 3-subgroup which is a subgroup of order 3. We must have that n_3 divides 4 and $n_3 \equiv 1 \mod 3$, so $n_3 = 1$ or $n_3 = 4$. In fact $n_4 = 4$ (verify!).

13.5. **Applications of Sylow's theorems.** We will use the Sylow theorems to say various things about groups given their orders.

Example 13.5.1. Suppose $|G| = 40 = 2^3 \times 5$. Then the number of Sylow 5-subgroups n_5 divides 8 and $n_5 \equiv 1 \mod 5$, so $n_5 = 1$. That is, there is only one subgroup of order 5 and by Corollary 13.4.9, it must be normal. The number of Sylow 2-subgroups (of order 8) n_2 must divide 5 and $n_2 \equiv 1 \mod 2$, so that n_2 can be 1 or 5. If $n_2 = 1$, the Sylow 2-subgroup must be normal. Otherwise, if $n_2 = 5$, the subgroup is not normal. Let H_5 be a subgroup of order 5 and H_2 a subgroup of order 8. Then H_5H_2 is a subgroup, has order 40 and hence must be equal to G. If H_2 is also normal, then $G = H_5 \times H_2$.

Example 13.5.2. Let $|G| = 30 = 2 \times 3 \times 5$. Then n_5 divides 6 and $n_5 \equiv 1 \mod 5$, so $n_5 = 1$ or 6; n_3 divides 10 and $n_3 \equiv 1 \mod 3$ so that $n_3 = 1$ or 10. We cannot have both 6 subgroups of order 5 and 10 subgroups of order 3 as $|G| = 30$. Hence one of the subgroups of order 3 or 5 (or both) is unique and hence normal in G. The product of the 3-Sylow subgroup, say H_3 and the 5-Sylow subgroup H_5 is a group H_3H_5 of order 15. We claim that H_3H_5 is cyclic and normal.

To see that it is cyclic, we apply Sylow's third theorem to the group H_3H_5. In particular, the number n_3' of 3-Sylow subgroups in H_3H_5 divides 5 and is congruent to 1 mod 3, forcing $n_3' = 1$. Similarly, n_5' divides 3 and $n_5' \equiv 1 \mod 5$, so $n_5' = 1$. Hence there exists an element of H_3H_5 of order 15 so that H_3H_5 is cyclic.

Next, we see that $|G : H_3H_5| = \frac{30}{15} = 2$, so H_3H_5 is normal. Now, $H_3H_5 = \langle a \rangle$ for some element a of order 15. The subgroup H_5 is also cyclic and $H_5 = \langle a^k \rangle$ for some $k \in \mathbb{N}$. Let $x \in G$. Then $x(a^k)^m x^{-1} = (xa^m x^{-1})^k = (a^r)^k$ for some r as $a^m \in H_3H_5$ which is normal. Now $(a^r)^k = (a^k)^r \in H_5$, so H_5 is indeed normal. Similarly, it can be shown that H_3 is also normal.

Finally, let x be an element of order 2. Then $G = \{x^i a^j \mid 0 \leq i \leq 1, 0 \leq j \leq 14\}$, where a is an element of order 15 as above.

Example 13.5.3. Suppose $|\,G\,| = 72 = 2^3 \times 3^2$. We will show that G has a proper non-trivial normal subgroup. Now n_3 divides 8 and $n_3 \equiv 1 \mod 3$, so $n_3 = 1$ or 4. If $n_3 = 1$, then the Sylow 3-subgroup H_3 is normal. Otherwise let H_3 and H_3' be two distinct Sylow 3-subgroups. Then $|\,H_3H_3'\,| = \frac{|\,H_3\,||\,H_3'\,|}{|\,H_3 \cap H_3'\,|} = \frac{81}{|\,H_3 \cap H_3'\,|}$. Since $|\,H_3 \cap H_3'\,|$ divides 9 and $H_3 \neq H_3'$, we must have $|\,H_3 \cap H_3'\,| = 3$ (think about why it cannot be 1!). Hence $|\,H_3H_3'\,| = \frac{81}{3} = 27$.

Now as $|\,H_3\,|, |\,H_3'\,| = 9 = 3^2$, they are Abelian (Theorem 9.4.1). Hence H_3 and H_3' are contained in $N(H_3 \cap H_3')$ so that $|\,N(H_3 \cap H_3')\,|$ divides 72, is divisible by 9 and has at least $|\,H_3H_3'\,| = 27$ elements. Hence $|\,N(H_3 \cap H_3')\,|$ is either 36 or 72. If it is the former, then $|\,G : N(H_3 \cap H_3')\,| = 2$, so the normalizer is normal. In the latter case, $N(H_3 \cap H_3') = G$, so that $H_3 \cap H_3'$ is normal in G.

The following theorem is useful in classifying groups of order pq where p and q are primes satisfying certain conditions.

Theorem 13.5.4. *If $|\,G\,| = pq$, where p and q are primes, $p < q$ and p does not divide $q - 1$, then G is cyclic. Hence $G \cong \mathbb{Z}_{pq}$.*

Proof. Let H_p be a Sylow p-subgroup of G and H_q be a Sylow q-subgroup of G. Now $n_p = 1 + kp$ for some $k \in \mathbb{Z}$ and n_p divides q, so that $n_p = 1$ or q. But n_p is not q as p does not divide $q - 1$. Hence $n_p = 1$.

Similarly, n_q divides p so it is 1 or p. On the other hand, $n_q = 1 + lq$ for some $l \in \mathbb{Z}$. If $n_q = p$, then q divides $p - 1$, a contradiction as $p < q$. Hence $n_p = 1 = n_q$, so that H_p and H_q are normal.

Let $H_p = \langle x \rangle$ and $H_q = \langle y \rangle$. We claim that $xy = yx$. Indeed, $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in H_qy^{-1} = H_q$ and similarly $xyx^{-1}y^{-1} \in H_p$. This implies that $xyx^{-1}y^{-1} \in H_p \cap H_q = \{e\}$, so that $xy = yx$. Hence $|\,xy\,| = pq$ and G is cyclic. □

Let's consider some implications of the above theorem. In fact, we use a great deal of knowledge built up so far about finite groups.

Example 13.5.5. Let $|\,G\,| = 99 = 3^2 \times 11$. Then n_{11} divides 9 and $n_{11} \equiv 1 \mod 11$, so $n_{11} = 1$ and the Sylow 11-subgroup H_{11} is normal. Similarly, the Sylow p-subgroup H_3 is normal. Now H_{11} is of order 11 and hence cyclic and Abelian (that is, $H_{11} \cong \mathbb{Z}_{11}$). The subgroup H_3 is of order 9 and hence Abelian; thus it is either isomorphic to $\mathbb{Z}_9$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Elements from H_3 and H_{11} commute with each other (verify this- the proof is similar to that in Theorem 13.5.4). As $H_3 \cap H_{11} = \{e\}$, we get that $G = H \times K$, so that G is also Abelian. Hence $G \cong \mathbb{Z}_{99}$ or $G \cong \mathbb{Z}_{33} \oplus \mathbb{Z}_3$.

Example 13.5.6. Let $|\,G\,| = 66 = 2 \times 3 \times 11$. Then as n_{11} divides 6 and $n_{11} \equiv 1 \mod 11$, we get $n_{11} = 1$ and H_{11} is normal in G. n_3 divides 22 and $n_3 \equiv 1 \mod 3$ implies that $n_3 = 1$ or 22.

Now $|\,H_3H_{11}\,| = \frac{3 \times 11}{|\,H_3 \cap H_{11}\,|} = 33$. As H_{11} is normal, H_3H_{11} is a subgroup of order 33. As 3 does not divide $11 - 1 = 10$, we can use Theorem 13.5.4 to get that H_3H_{11} is cyclic, say $\langle x \rangle$. Now, let $y \in G$ be any element of order 2 which is sure to exist by Cauchy's theorem. As $\langle x \rangle$ is normal (as it has index 2), $yxy^{-1} = x^i$ for some $i \in \{1, \ldots, 32\}$. We will now identify the possible values for i. It is not hard to see that as $x^i = yxy^{-1}$, $\left|\,x^i\,\right| = |\,x\,| = 33$, hence

$\gcd(i, 33) = 1$. Also,

$$\begin{aligned} x &= y^{-1}(yxy^{-1})y \\ &= y^{-1}x^i y \\ &= yx^i y^{-1} \\ &= (yxy^{-1})^i \\ &= (x^i)^i \\ &= x^{i^2}. \end{aligned}$$

Hence 33 divides $i^2 - 1$ and so 11 divides $i \pm 1$, so that $i = 0 \pm 1, 11 \pm 1, 22 \pm 1$ or 33 ± 1. Consolidating all the conditions on i, we get $i = 1, 10, 23$ or 32, so that there are at most 4 groups of order 66.

Finally, we can check that there are exactly 4 as the following are all non-isomorphic groups of order 66:

$\mathbb{Z}_{66}$
D_{33}
$D_{11} \oplus \mathbb{Z}_3$
$D_3 \oplus \mathbb{Z}_{11}$.

Example 13.5.7. Let $|\, G \,| = 255 = 3 \times 5 \times 17$. Then n_{17} divides 15 and $n_{17} \equiv 1 \mod 17$ so that $n_{17} = 1$. Hence H_{17} is normal, so $N(H_{17}) = G$.

Now $\left| {}^{N(H_{17})}\!/_{C(H)_{17}} \right|$ divides $|\, \mathrm{Aut}(H_{17}) \,| = |\, U(17) \,| = 16$ by Example 10.3.3. (iii). Hence $\left| {}^{G}\!/_{C(H_{17})} \right|$ divides 16 and 255 so must be equal to 1. This implies that $C(H_{17}) = G$ so that $H_{17} \subseteq Z(G)$. Hence 17 divides $|\, Z(G) \,|$ and $|\, Z(G) \,|$ divides 255, so $|\, Z(G) \,| = 17, 51, 85$ or 255. This gives that $\left| {}^{G}\!/_{Z(G)} \right| = 15, 5, 3$ or 1. In all cases, ${}^{G}\!/_{Z(G)}$ is cyclic, so G is Abelian and hence isomorphic to $\mathbb{Z}_{255}$.

References

[1] Chapter 24. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.