Chapter 25 Finite Simple Groups

Historical Background

Definition A group is simple if it has no nontrivial proper normal subgroup.

- The definition was proposed by Galois; he showed that A_n is simple for $n \geq 5$ in 1831.
- It is an important step in showing that one cannot express the solutions of a quintic equation in radicals.
- If possible, one would factor a group G as $G_0 = G$, find a normal subgroup G_1 of maximum order to form G_0/G_1. Then find a maximal normal subgroup G_2 of G_1 and get G_1/G_2, and so on until we get the composition factors: $G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n$, with $G_n = \{e\}$.
- Jordan and Hölder proved that these factors are independent of the choices of the normal subgroups in the process.
- Jordan in 1870 found four infinite series including: $\mathbb{Z}_p$ for a prime p, $SL(n, \mathbb{Z}_p)/Z(SL(n, \mathbb{Z}_p))$ except when $(n, p) = (2, 2)$ or $(2, 3)$.
- Between 1982-1905, Dickson found more infinite series; Miller and Cole showed that 5 (sporadic) groups constructed by Mathieu in 1861 are simple.

- In 1950s, more infinite families were found, and the classification project began.
- Brauer observed that the centralizer has an order 2 element is important; Feit-Thompson in 1960 confirmed the 1900 conjecture that non-Abelian simple group must have even order.
- From 1966-75, 19 new sporadic groups were found.
- Thompson developed many techniques in the N-group paper.
- Gorenstein presented an outline for the classification project in a lecture series at University of Chicago in 1972.
- Aschbacher and Fischer further developed the techniques of Thompson.
- Then Griess construct the monster group with about $8 \cdot 10^{53}$ elements represented as matrices in M_{196883}.
- In 2004, it was announced that the classification was completed.
- There are 18 countable series, and 26 sporadic groups. [1]

[1] The Tits group in one of the series is also referred to as the 27th sporadic group by some researchers.

Theorem 25.1 If G is a finite group with $|G| = n$, which is a composite number, and p be a prime factor of n. If 1 is the only divisor of n that is equal to 1 modulo p, then G is not simple.

Proof. If n is a prime power, then the center of G is a non-trivial, and there will be a normal subgroup.
If $n = p^r m$ such that $p \not| m$, then the assumption implies that the Sylow p-subgroup is normal. □

Remark Try $n = 4, 8, 9, 10, \ldots$.

From 1 to 200, simple groups could only have the following orders:

12, 24, 30, 36, 48, 56, 60, 72, 80, 90, 96, 105, 108, 112, 120, 132, 144, 150, 160, 168, 180, 192.

In fact, Theorem 25.1 can be used to rule out 90% of the numbers from 1 to n if $n \geq 500$.

Theorem 25.2 If G is a finite group with $|G| = n = 2(2k+1)$, where $k \geq 1$. Then G is not simple.

Proof. Consider the map from G to S_G defined by $g \mapsto T_g$ such that $T_g(x) = gx$. Now, G has an element g of order 2 so that T_g is a product of length 2 and length 1 cycles. However, T_g has no 1-cycle, else, $T_g(x) = gx = x$ implies that $g = e$. Thus, T_g is a product of $(2k+1)$ cycles. Thus, set of elements in G corresponds to even permutations in S_G is a normal subgroup of index 2. Thus, it is a normal subgroup of G. □

Theorem 25.3 [Generalized Cayley Theorem] Suppose $H < G$. Let S be the group of all permutation of the left cosets of H in G. Then $\phi : G \to S$ defined by $\phi(g) = T_g$ such that $T_g(xH) = gxH$ is a group homomorphism. The kernel of ϕ lies in H and contains every normal subgroup of G that is contained in H.

Proof. Every $g \in G$ induces a permutation T_g of the cosets xH of H by the action $T_g(xH) = gxH$.
Now, $\phi : G \to S$ defined by $\phi(g) = T_g$ is a group homomorphism, and $g \in \text{Ker}(\phi)$ implies that T_g is the identity map so that $H = T_g(H) = gH$. Thus, $g \in H$. So, $\text{Ker}(\phi) \subseteq H$.
Moreover, for any normal subgroup K of G lying in H and $k \in K$, we have $T_k(xH) = kxH = x\hat{k}H = xH$. Thus, $k \in \text{Ker}(\phi) \subseteq H$. □

Corollary 1 [Index Theorem] If G is a finite group and H is a proper subgroup of G such that $|G|$ does not divide $|G:H|!$, then H contains a non-trivial normal subgroup of G. So, G is not simple.

Proof. Suppose ϕ is defined as in the proof of Theorem 25.3. Then $\text{Ker}(\phi)$ is normal in G contained in H, and $G/\text{Ker}(\phi)$ is isomorphic to a subgroup of S. Thus, $|G/\text{Ker}(\phi)| = |G|/|\text{Ker}(\phi)|$ divides $|S| = |G:H|!$. Since $|G|$ does not divide $|G:H|!$, the order of $\text{Ker}(\phi)$ must be greater than 1. □

Corollary 2 [Embedding Theorem] If a finite non-Abelian simple group G has a subgroups of index n, then G is isomorphic to a subgroup of A_n.

Proof. Let H be the subgroup of index n, and let S_n be the group of all permutations of the n left cosets of H in G. By Theorem 25.3, there is a non-trivial homomorphism from G into S_n.
Since G is simple and the kernel of a homomorphism is a normal subgroup of G, we see that the mapping from G into S_n is one-to-one, so that G is isomorphic to some subgroup of S_n.
So, $G \cap A_n = G$ or $G \cap A_n$ is a subgroup of index 2. □

Further elimination of possible orders of simple groups

By the Index Theorem, we can further eliminate the possible orders of simple groups.

Example If $|G| = 80$, then 16 does not divide $5!$. So, G is not simple.

Same argument applies to $|G| = 12, 24, 36, 48, 96, 108, 160, 192$.

We are left with: 56, 60, 72, 105, 112, 120, 132, 144, 168, and 180.

Example For $56 = 8 \cdot 7$, assume that there are 8 7-element subgroups, and 7 8-element subgroups. Then we get $8 \cdot 6$ order 7 elements, and at least $8 + 8 - 4 = 12$ different elements in the union of 2 8-element subgroups, which is too many.

Similarly, we can get rid of 105, 132.

Further techniques

We are left with 60, 72, 112, 120, 144, 168, 180.

Of course, A_5 has 60 element is simple. To show that A_5 is simple, assume that A_5 has nontrivial proper subgroup H. Then $|H|$ can be 2,3,4,5,6,10,12,15,20,30.

Now, A_5 has 24 elements of order 5, 20 elements of order 3, no elements of order 15.

If $|H|$ is $3, 6, 12, 15$, then $|A_5/H|$ is relatively prime to 3 so that all 20 order 3 elements will be in H!

If $|H|$ is $5, 10, 20$, then $|A_5/H|$ is relatively prime to 5 so that all 24 order 5 elements will be in H!

If $|H| = 30$, then $|A_5/H|$ is relatively prime to 3 and 5 so that all the order 3 and 5 elements will be in H!

If $H| = 2$ or 4, then $|A_5/H| = 30$ or 15. Then A_5/H has an element of order 15 implying A_5 has an element of order 15, a contradiction.

Similarly, one can show that $SL(2, \mathbb{Z}_7)/Z(SL(2, \mathbb{Z}_7))$ has 168 (?) elements is simple.