Algebra 2. Groups of order ≤ 100 .

In this note we show that the only non-commutative simple group of order ≤ 100 is the alternating group A_5 of order 60.

Lemma 1. Let G be a non-commutative simple group of order n. Let p be a prime dividing n and let m be the number of p-Sylow subgroups. Then G is isomorphic to a subgroup of S_m . In particular, n divides m!.

Proof. Since G is simple but not commutative, we have m > 1. The action by conjugation of G on its p-Sylow subgroups leads to a homomorphism $i: G \longrightarrow S_m$. Since the action of G is transitive, the image of i is a non-trivial subgroup of S_m . It follows that i is injective and the Lemma follows.

Proposition 2. Let G be a group of order n. In the following cases G admits a proper normal subgroup:

- (a) n = 2m with m > 1 odd;
- (b) $n = p^k$ where p is prime and $k \ge 2$;
- (c) n = pq where p and q are primes;
- (d) $n = p^2 q$ where p and q are primes;
- (e) n = 8p with p prime.

Proof. (a) Let $x \in G$ be an element of order 2. The permutation $G \longrightarrow G$ induced by left multiplication by x is a product of m disjoint 2-cycles. Therefore it is odd. The kernel of the surjective homomorphism

$$G \longrightarrow S(G) \xrightarrow{\text{sign}} \{\pm 1\}$$

is a normal subgroup of index 2 of G.

(b) This is clear when G is commutative. In the other cases the center of G is a proper normal subgroup.

(c) If p = q this follows from (b). In the other cases, either the *p*-Sylow subgroup or the *q*-Sylow subgroup is unique and hence normal. Indeed, if not, we have $p \ge q + 1$ as well as $q \ge p + 1$, which is impossible.

(d) If p = q this follows from (b). In the other cases, either the *p*-Sylow subgroup or the *q*-Sylow subgroup is unique and hence normal. Indeed, the number of *q*-Sylow subgroups is 1, *p* or p^2 . If it is p^2 , then the cardinality of the complement of the subset of elements of order *q* is $p^2q - p^2(q-1) = p^2$. This shows that there can be only one *p*-Sylow subgroup. If the number of *q*-Sylow subgroups is *p* and the *p*-Sylow subgroup is not unique, we have $p \ge q + 1$ as well as $q \ge p + 1$, which is impossible.

(e) If p = 2 the result follows from (b). If p > 2 and the *p*-Sylow subgroup of *G* is unique, it is normal and we are done. Suppose it is not unique. Then their number *m* divides 8. Since $m \equiv 1 \pmod{p}$, this implies that p = 3 or 7. If p = 7, there are eight 7-Sylow subgroups and the complement of the subset of elements of order 7 is 56 - 8(7 - 1) = 8, showing that the 2-Sylow subgroup is normal. If p = 3, there are four 3-Sylow subgroups. If *G* were simple, then Lemma 1 shows $G \cong S_4$, a contradiction.

Proposition 3. Any non-commutative simple group of order ≤ 100 has order 60.

Proof. Let G be a non-commutative simple group of order ≤ 100 . Since groups of prime order are commutative, Proposition 2 implies easily that $n \in \{36, 48, 60, 72, 84, 80, 96, 100\}$.

If n = 84, the 7-Sylow subgroup of G is normal and if n = 100 the 5-Sylow subgroup of G is normal. This follows from Sylow's theorems. If n = 36 or 72, there are exactly four 3-Sylow subgroups. If n = 48 or 96, there are precisely three 2-Sylow subgroups. If n = 80 there are five 2-Sylow subgroups. In each case this contradicts Lemma 1.

Proposition 4. A simple group of order 60 is isomorphic to A_5 .

Proof. Let G be a simple group of order 60. Consider the 2-Sylow subgroups of G. They have order 4 and their number m divides 15. Since G is simple, Lemma 1 implies that m is not equal to 1 or 3. If m = 5, Lemma 1 provides us with an injective homomorphism $G \longrightarrow S_5$.

Suppose that m = 15. Since G admits six 5-Sylow subgroups, the complement of the set of elements of order 5 has 60 - 6(5 - 1) = 36 elements. Therefore there are at least two 2-Sylow subgroups P and P' with non trivial intersection. Let $1 \neq x \in P \cap P'$ and let H be the centralizer of x. Since P' centralizes x, the group P is a proper subgroup of H. It follows that $\#H \ge 12$ and hence $k = [G:H] \le 5$. Translation by G of the cosets of H induces a non-trivial and hence injective homomorphism $G \longrightarrow S_k$. It follows that k = 5.

So both when m = 5 and m = 15, we obtain an injective homomorphism $G \longrightarrow S_5$. Since A_5 does not admit a subgroup of index 2, we have $G \cong A_5$ as required.

2