Uniquely Simple

Theorem: Let G be a simple group with $|G| > 2$ and assume G acts on a finite set X.
Then G acts as even permutations on X.

Proof: Let G acts on X. We then have the corresponding permutation representation $\varphi : G \to S(X)$ where $\varphi(g)[x] = g \bullet x$. Since G is simple $\mathrm{Ker}(\varphi)$ must be $\{1\}$ or G. If $\mathrm{Ker}(\varphi) = G$, then G acts trivially: each element acts as the identity permutation (1) (which is even). On the other hand, suppose $\mathrm{Ker}(\varphi) = \{1\}$. Then by the first isomorphism theorem, $G \cong \varphi(G)$ a subgroup of $S(X)$. Recall that subgroups of $S(X)$ are either even or half-even and half-odd. Thus either $\varphi(G)$ is even (done) or $\varphi(G)$ is half-even and half-odd. We show the latter case is impossible. If $\varphi(G)$ is half-even, then $\varphi(G)$ intersected with the subgroup of even permutations in $S(X)$ yields a subgroup of $\varphi(G)$ of index 2. By the index 2 theorem, this is a normal subgroup of $\varphi(G)$. But $|G| > 2$ so this is a non-trivial (proper) normal subgroup contradicting the assumption that G is simple. ∎

Corollary: Let G be a non-Abelian simple group. Suppose G has a subgroup of (finite) index $k > 1$. Alternatively, suppose G acts non-trivially on a set of size k. Then G is isomorphic to a subgroup of A_k where $k \geq 5$.

Proof: Non-Abelian implies $|G| > 2$. Let H be a subgroup of G of index $[G : H] = k$. Then G acts non-trivially (by left multiplication) on the (left) cosets of H in G: $g \bullet xH = (gx)H$. Thus G acts non-trivially on a set of size $[G : H] = k$ and so G is isomorphic to a subgroup of A_k. Finally, the alternating groups A_k for $k < 5$ do not contain non-Abelian simple groups (A_2 is trivial, A_3 is cyclic order 3, and A_4 is not simple and its proper subgroups are Abelian). Therefore, $k \geq 5$. ∎

It turns out that there are many interesting *infinite* simple groups (which are necessarily non-Abelian). The above corollary implies that infinite simple groups cannot have subgroups of finite index.

Example: There are no simple groups of order $80 = 2^4 \cdot 5$. Suppose G is such a group. By the third Sylow theorem, the number of Sylow 2-subgroups, n_2, must divide 5. Since G is simple, $n_2 \neq 1$ (otherwise, the unique Sylow 2-subgroup would be a proper non-trivial normal subgroup). Therefore, $n_2 = 5$. Now G acts on the set of Sylow 2-subgroups via conjugation. By the second Sylow theorem, this action has a single orbit. Thus it is a non-trivial action on set of size 5. Therefore, G must be isomorphic to a subgroup of A_5. But this is impossible since $|G| = 80 > |A_5| = 60$.

Theorem: There is a unique (up to isomorphism) simple group of order 60, namely A_5.

Proof: Let G be simple and $|G| = 60 = 2^2 \cdot 3 \cdot 5$. Let $\mathcal{S}$ denote the set of Sylow 2-subgroups of G and let $n_2 = |\mathcal{S}|$. The third Sylow theorem says that $n_2 \equiv 1 \pmod 2$ and n_2 divides 15. Therefore, n_2 is either 1, 3, 5, or 15. Since G is simple, $n_2 \neq 1$ (otherwise the unique Sylow 2-subgroup would be normal contradicting the simplicity of G).

Recall that G acts on $\mathcal{S}$ via conjugation (the conjugate of a Sylow 2-subgroup is a Sylow 2-subgroup). Also, the second Sylow theorem says that this action is transitive (i.e., all of $\mathcal{S}$ is a single orbit). Thus since $|\mathcal{S}| = n_2 > 1$, this is a non-trivial action. So G is a simple group which acts non-trivially on a set of size n_2.

If $n_2 = 3$, the theorems above would imply that G is isomorphic to a subgroup of A_3. But this is impossible since G is too big: $|G| = 60 > 3 = |A_3|$. If $n_2 = 5$, the same theorems would imply that G is isomorphic to a subgroup of A_5, say $G \cong \overline{G} \subseteq A_5$. But $|G| = |\overline{G}| = 60$ and $|A_5| = 60$ so $G \cong \overline{G} = A_5$ (and we would be done).

We now turn to the only remaining case: $n_2 = 15$. Let $P \in \mathcal{S}$. Then $[G : N_G(P)] = n_2 = 15$ where $N_G(P) = \{g \in G \mid gxg^{-1} \in P \text{ for all } x \in P\}$ is the normalizer of P in G. Thus $|N_G(P)| = 60/15 = 4$ and since $P \subseteq N_G(P)$ where $|P| = 4$ (since P is a Sylow 2-subgroup) we must have $P = N_G(P)$ (i.e., P is "self-normalizing").

Let $x \in G$ be an element of order 2 (these exist by Cauchy's theorem). Notice that $xPx^{-1} = P$ if and only if $x \in N_G(P) = P$. By the second Sylow theorem, $\langle x \rangle$ (a subgroup of order 2) must be contained in some Sylow 2-subgroup, say P. Consider x acting on $\mathcal{S}$ via conjugation: x fixes P. Since x's order is 2, it can either fix or exchange pairs of elements in $\mathcal{S}$. If x did not fix any element of $\mathcal{S}$ other than P, it would act as a permutation consisting of a 1-cycle and 7 (disjoint) transpositions (since $|\mathcal{S}| = 15$). This would mean that x acted as an odd permutation. But by our theorem this is impossible since G is simple. Therefore, x must fix at least one other Sylow 2-subgroup, say Q and so $x \in N_G(Q) = Q$. Therefore, $x \in P \cap Q$. Since P and Q are distinct, order 4, and share 1 and x, we have $|P \cap Q| = 2$ (i.e., $P \cap Q = \langle x \rangle = \{1, x\}$).

Now consider $N = N_G(P \cap Q)$. Now P and Q are of order 4, thus they are Abelian. Therefore, $P \cap Q$ is not just a subgroup but a normal subgroup of both P and Q. Therefore, we have both P and Q are contained in N (the normalizer of $P \cap Q$). Therefore, $|N| \geq |P \cup Q| \geq 6$ and since P is a subgroup of N and N is a subgroup of G, $|N|$ must be a multiple of 4 and a divisor of 60. Thus $|N| = 12, 20$, or 60. We cannot have $|N| = 60$ since otherwise, $N_G(P \cap Q) = N = G$ which means $P \cap Q$ is a non-trivial (since $|P \cap Q| = 2$) proper normal subgroup (contradicting the simplicity of G). If $|N| = 20$, then $[G : N] = 60/20 = 3$ and so G would necessarily be isomorphic to a subgroup of A_3 (this is impossible since G is too big). Therefore, $|N| = 12$. Thus $[G : N] = 60/12 = 5$. Therefore, G is isomorphic to a subgroup of A_5. Again, since G has order $60 = |A_5|$, this subgroup must be all of A_5.

Therefore, in all cases, we must conclude that $G \cong A_5$. ∎