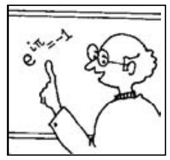

In this section of *Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

A Note on the Converse of Lagrange's Theorem

Dinesh Khurana
Department of Mathematics
Punjab University
Chandigarh 160 014, India.
Email: dkhurana@pu.ac.in

Lagrange's theorem which is one of the most important theorems of group theory tells us that if a finite group G has a subgroup H, then the order of H divides the order of G. Does this proposition have a converse? The answer is No, but generally one sees the same counterexample in all expositions. This article provides more counterexamples, and demonstrates that they are counterexamples in an elementary way.

One of the most important theorems in finite group theory is the following.

Theorem 1 (Lagrange). *The order of a subgroup divides the order of the group.*

The following natural question arises: Is the converse of Lagrange's theorem true? That is: *If d is a divisor of the order of G, then does G necessarily have a subgroup of order d?*

Cauchy's theorem says that the converse does hold for prime values of d and, more generally, Sylow's theorem says that it holds for prime power values of d.

Keywords
Finite group, subgroup, Lagrange's theorem converse, alternating group.

A group of order 12 is the smallest group for which the converse of Lagrange's theorem fails.

The standard example of the alternating group A_4, which has order 12 but has no subgroup of order 6, shows that the converse of Lagrange's theorem is not true. We could not find an undergraduate text which gives some other counterexample. One possible reason is that a group of order 12 is the smallest group for which the converse of Lagrange's theorem fails. Because smaller groups have one of the following orders: 1, p^n, pq, where p, q are distinct primes, implying that any proper divisor of the order of such a group is either a prime or a power of a prime, for such groups the converse does hold in view of Sylow's theorem.

One wonders whether there are other elementary examples to demonstrate the failure of the converse of Lagrange's theorem. Indeed there are many. The following result whose proof is an extension of Gallian's proof [1] of the fact that A_4 has no subgroup of order 6, gives many easy examples of the failure of the converse of Lagrange's theorem.

Proposition 2. *If $n > 4$, then A_n has no subgroup of order $n!/4$.*

Proof. If H is a subgroup of order $n!/4$, then H has only two left cosets in A_n. So if a is a 3-cycle in A_n, then the cosets H, aH, a^2H cannot be all distinct. Equality of any two of the above cosets implies either $a \in H$ or $a^2 \in H$. Now $a^2 \in H$ implies $a = a^4 \in H$. Thus H contains all 3-cycles. Now A_n is generated by 3-cycles; indeed we have $(12)(23) = (123)$ and $(12)(34) = (124)(134)$. It follows that $H = A_n$, a contradiction. □

The result in Proposition 2 follows for $n > 4$ from the simplicity of A_n, but this result is generally proved much after Lagrange's theorem.

The above result also follows for $n > 4$ from the simplicity of A_n, but this result is generally proved much after Lagrange's theorem. Moreover if we assume the simplicity of A_n for $n > 4$, then we can actually prove that for $1 < k < n$ there is no subgroup of index k in A_n. That is, A_n has no subgroup of order $n!/(2k)$ for any $1 < k < n$, though $n!/(2k)$ is a divisor of the order of A_n. For this we need the following lemma whose proof is left to the reader.

The converse of Lagrange's theorem does hold for groups whose every subgroup is normal.

Lemma 3. *Let S be the set of all right cosets of a subgroup H in a group G and let $g \in G$. Then the right multiplication ρ_g by g is a permutation on S, i.e., $\rho_g \in A(S)$, the group of permutations on S. Moreover $g \longmapsto \rho_g$ is a group homomorphism from $G \to A(S)$ whose kernel is contained in H.*

Theorem 4. *If $n > 4$ and $1 < k < n$, then A_n has no subgroup of order $n!/(2k)$.*

Proof. Assume to the contrary that for some $n > 4$ and some $1 < k < n$, H is a subgroup of order $n!/(2k)$ of $G = A_n$. Since A_n is simple for $n > 4$, the map $g \longmapsto \rho_g$ defined in the Lemma is a monomorphism. So the order of A_n divides $i(H)!$, where $i(H)$ denotes the index of H in G. Now as $i(H)! = k!$, it follows that $n!/2$ divides $k!$. As $n!/2 > k!$, this gives the desired contradiction. $\square$

It is easy to show that the converse of Lagrange's theorem holds for groups whose every subgroup is normal. Indeed, let d be a proper divisor of the order of such a group G and p be a prime divisor of d. Let H be a subgroup of G of order p. Then d/p is a divisor of the order of G/H. As every subgroup of G/H is also normal, by induction, G/H has a subgroup, say K/H, of order d/p. Then K is a subgroup of G of order d. In particular, the converse of Lagrange's theorem holds for abelian groups.