3.5 Applications of Lagrange's Theorem

Before coming to our next remark, we need the following definition and example.

Definition 3.5.1 (Order of an Element)**.** *Let G be a group and let $g \in G$. Then* **the smallest positive integer** *m such that $g^m = e$ is called the order of g. If there is no such positive integer then g is said to have* **infinite order***. The order of an element is denoted by $\mathbf{O}(g)$.*

Example 3.5.2. *1. The only element of order 1 in a group G is the identity element of G.*

2. In D_4, the elements r^2, f, rf, r^2f, r^3f have order 2, whereas the elements r and r^3 have order 4.

With the definition of the order of an element, we now prove that in general, the converse of Lagrange's Theorem is not true. To see this consider the group G discussed in Example 3.2.1.2a. This group has 12 elements and 6 divides 12. Whereas it can be shown that G doesn't have a subgroup of order 6. We give a proof for better understanding of cosets.

Proof. Let if possible, H be a subgroup of order 6 in G, where

$$G = \{e, (234), (243), (124), (142), (123), (132), (134), (143), (12)(34), (13)(24), (14)(23)\}.$$

Observe that G has exactly 8 elements of the form (ijk), for distinct numbers i, j and k, and each has order 3. Hence, G has exactly 8 elements of order 3. Let $a \in G$ with $\mathbf{O}(a) = 3$. Then using Theorem 3.4.5, we see that cosets of H in G will be exactly 2 and at the same time, the possible cosets could be H, aH and a^2H (as $a^3 = e$, no other coset exists). Hence, at most two of the cosets H, aH and a^2H are distinct. But, using Theorem 3.4.5, it can be easily verified that the equality of any two of them gives $a \in H$. Therefore, all the 8 elements of order 3 must be elements of H. That is, H must have at least 9 elements (8 elements of order 3 and one identity). This is absurd as $|H| = 6$. ■

We now derive some important corollaries of Lagrange's Theorem. We omit the proof as it can be found in any standard textbook in abstract algebra. The first corollary is about the order of an element of a finite group. The observation that for each $g \in G$, the set $H = \{e, g, g^2, g^3, \ldots\}$ forms a subgroup of any finite group G gives the proof of the next result.

Corollary 3.5.3. *Let G be a finite group and let $g \in G$. Then $\mathbf{O}(g)$ divides $|G|$.*

Remark 3.5.4. *Corollary 3.5.3 implies that if G is a finite group of order n then the possible orders of its elements are the divisors of n. For example, if $|G| = 30$ then for each $g \in G$, $\mathbf{O}(g) \in \{1, 2, 3, 5, 6, 10, 15, 30\}$.*

Let G be a finite group. Then in the first corollary, we have shown that for any $g \in G$, $\mathbf{O}(g)$ divides $|G|$. Therefore, $|G| = m \cdot \mathbf{O}(g)$, for some positive integer m. Hence

$$g^{|G|} = g^{m \cdot \mathbf{O}(g)} = (g^{\mathbf{O}(g)})^m = e^m = e.$$

This observation gives our next result.

Corollary 3.5.5. *Let G be a finite group. Then, for each $g \in G, g^{|G|} = e$.*

Let P be an odd prime and consider the set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$. Then, check that $\mathbb{Z}_p^*$ forms a group with respect to the binary operation

$$a \odot b = \text{the remainder, when } ab \text{ is divided by } p.$$

Applying Corollary 3.5.5 to $\mathbb{Z}_p^*$ gives the famous result called the *Fermat's Little Theorem*. To state this, recall that for $a, b \in \mathbb{Z}$, the notation "$a \equiv b \pmod{p}$" indicates that p divides $a - b$.

Corollary 3.5.6. *Let a be any positive integer and let p be a prime. Then $a^{p-1} \equiv 1 \pmod{p}$, if p does not divide a. In general, $a^p \equiv a \pmod{p}$.*

We now state without proof a generalization of the Fermat's Little Theorem, popularly known as the Euler's Theorem. to do so, let $U_n = \{k : 1 \leq k \leq n, \gcd(k, n) = 1\}$, for each positive integer n. Then U_n, with binary operation

$$a \odot b = \text{the remainder, when } ab \text{ is divided by } n$$

forms a group. Also, recall that the symbol $\varphi(n)$ gives the number of integers between 1 and n that are coprime to n. That is, $|U_n| = \varphi(n)$, for each positive integer n. Now applying Corollary 3.5.5 to U_n, gives the next result.

Corollary 3.5.7. *Let $a, n \in \mathbb{Z}$ with $n > 0$. If $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Example 3.5.8. *1. Find the unit place in the expansion of 13^{1001}.*

Solution : *Observe that $13 \equiv 3 \pmod{10}$. So, $13^{1001} \equiv 3^{1001} \pmod{10}$. Also, $3 \in U_{10}$ and therefore by Corollary 3.5.5, $3^{|U_{10}|} = 1 \pmod{10}$. But $|U_{10}| = 4$ and $1001 = 4 \cdot 250 + 1$. Thus,*

$$13^{1001} \equiv 3^{1001} \equiv 3^{4 \cdot 250 + 1} \equiv (3^4)^{250} \cdot 3^1 \equiv 1 \cdot 3 \equiv 3 \pmod{10}.$$

Hence, the unit place in the expansion of 13^{1001} is 3.

2. Find the unit and tens place in the expansion of 23^{1002}.

Solution : *Observe that $23 \in U_{100}$ and $23^{|U_{100}|} = 1 \pmod{100}$. But $|U_{100}| = 40$ and $1002 = 40 \cdot 25 + 2$. Hence*

$$23^{1002} \equiv 23^{40 \cdot 25 + 2} \equiv (23^{40})^{25} \cdot 23^2 \equiv 1 \cdot 23^2 \equiv 529 \equiv 29 \pmod{100}.$$

Hence, the unit place is 9 and the tens place is 2 in the expansion of 23^{1002}.