WILSON’S THEOREM FOR FINITE FIELDS

Mehdi Hassani

In this short note, we introduce an analogue of Wilson’s theorem for all nonzero elements of a finite field, which reproves Wilson’s theorem and yields some Wilson type identities. Finally, we obtain an analogue of Wolstenholme’s theorem for nonzero elements of a finite field.

Let \( F \) be a finite field with \( \text{char}(F) = p \) and set \( |F| = p^n = q \). So, \( |F^*| = q - 1 \) where \( F^* = F - \{0\} = \{a_1, a_2, \ldots, a_{q-1}\} \). By Lagrange’s theorem, if \( a \in F^* \) then \( o(a)|q - 1 \) and so \( a^{q-1} = 1 \) or \( a^q = a \). This equation holds also for \( a = 0 \). Therefore, the elements of \( F \) are the roots of \( x^q - x \). However, this polynomial has at most \( q \) roots, so the elements of \( F \) are precisely the roots of \( x^q - x \). Thus, we obtain:

\[
x^q - x = x(x^{q-1} - 1) = \prod_{i=1}^{q-1} (x - a_i).
\]

Note that \( a_i \neq 0 \) for \( i = 1, 2, \ldots, q - 1 \) and we let \( q \geq 3 \). Considering elementary symmetric functions Morandi [2]:

\[
s_k = s_k(a_1, a_2, \ldots, a_{q-1}) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq q-1} a_{i_1}a_{i_2}\cdots a_{i_k},
\]

we have

\[
x^{q-1} - 1 = (x - a_1)(x - a_2)\cdots(x - a_{q-1})
\]

\[
= x^{q-1} - s_1 x^{q-2} + s_2 x^{q-3} + \cdots + (-1)^{q-1} s_{q-1},
\]

or the following identity:

\[
\sum_{k=1}^{q-1} (-1)^k s_k x^{q-1-k} + 1 = 0 \quad (x \in K^*),
\]

where \( K \) is a field extension of \( F \), and comparing coefficients, we obtain

\[
s_1 = 0, s_2 = 0, \ldots, s_{q-2} = 0 \text{ and } s_{q-1} = (-1)^{q-1} a_1 a_2 \cdots a_{q-1}.
\]
which we can state all of them together as follows:

\[ s_k = \left\lfloor \frac{k}{q-1} \right\rfloor (-1)^q \quad (k = 1, 2, \ldots, q-1 \text{ and } q \geq 3). \]

This relation is a generalization of the Wilson’s theorem for nonzero elements of a finite field. Specially, letting \( F = \mathbb{Z}_p \) with \( p \geq 3 \), we obtain

\[ \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq p-1} i_1 i_2 \cdots i_k \equiv -\left\lfloor \frac{k}{p-1} \right\rfloor \pmod{p}, \]

where \( k = 1, 2, \ldots, p-1 \) and putting \( k = p-1 \), it reproves Wilson’s theorem Apostol [1]; \( (p-1)! \equiv -1 \pmod{p} \).

Moreover, above mentioned results assert us to calculate the summations

\[ \sum_{k=1}^{q-1} \Phi(a_1, a_2, \ldots, a_{q-1}), \]

where \( \Phi \) is a symmetric function of \( a_1, a_2, \ldots, a_{q-1} \); because for above given \( \Phi \), there exists the function \( \Psi \), such that:

\[ \Phi(a_1, a_2, \ldots, a_{q-1}) = \Psi(s_1, s_2, \ldots, s_{q-1}) = \Psi(0, 0, \ldots, 0, s_{q-1}). \]

For example

\[ \sum_{k=1}^{q-1} \frac{a_1 a_2 \cdots a_{q-1}}{a_k} = (-1)^{q-2} s_{q-2} = 0 \quad (q \geq 5), \]

which is an analogue of Wolstenholme’s theorem Apostol [1]; \( \sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2} \) and \( p \geq 5 \).

**Acknowledgment.** I deem my duty to express my gratitude to Prof. Patrick Morandi and Dr. Robin Chapman for their valuable guidance and comments.

**REFERENCES**