Časopis pro pěstování matematiky a fysiky

L. Rédie

A short proof of a theorem of Št. Schwarz concerning finite fields

Časopis pro pěstování matematiky a fysiky, Vol. 75 (1950), No. 4, 211--212

Persistent URL: http://dml.cz/dmlcz/122665

Časopis pro pěstování matematiky a fysiky, roč. 75 (1950)

A SHORT PROOF OF A THEOREM OF ŠT. SCHWARZ CONCERNING FINITE FIELDS.

L. RÉDEI, Szeged (Hungary).

(Received January 23th, 1950.)

SCHWARZ[1]) recently proved a theorem concerning the important problem of factorization of binomal polynomials in finite fields. He also gave[1]) interesting applications of his theorem, especially a generalization of the VINOGRADOV'S estimation of the least primitive root mod p. The theorem mentioned above is as follows:[2])

Let K be a finite field of characteristic p having P elements. Then the polynomial

$$x^m - a \quad (a \neq 0, \in K;\ p \nmid m) \tag{1}$$

has in the field K just

$$\frac{1}{k} \sum_{t/k}' \mu\left(\frac{k}{t}\right) d_t \quad (d_t = (m, P^t - 1)) \tag{2}$$

irreducible factors of degree k, the summation being extended over all t with

$$a^{d'_t} = 1 \quad \left(d'_t = \frac{P^t - 1}{d_t}\right) \tag{3}$$

and $\mu(t)$ being the MÖBIUS function.

In what follows I give an elegant proof of this important theorem. The proof is based upon a Lemma which — as far as I am informed — is unknown in the formulation given here.

Lemma. The greatest common divisor of the polynomials

$$x^m - a,\ x^n - b \quad (a, b \neq 0;\ m, n \geqq 1) \tag{4}$$

in an arbitrary field has the degree 0 or $d = (m, n)$. The second case occurs, if and only if the relation

$$a^{\frac{n}{d}} = b^{\frac{m}{d}} \tag{5}$$

holds.

[1]) ŠT. SCHWARZ: On the reducibility of binomial congruences and on the bound of the least integer belonging to a given exponent mod p, Časopis pro pěst. mat. a fys., **74** (1949), p. 1—16.

[2]) L. c. p. 2 (Theorem 1) and p. 13 (Generalization of Theorem 1).

The statement is true, if $m = n$. (Hence, it is true if $m + n = 2$.) In the remaining case we prove it by induction. Let us suppose that it is true for all couples of polynomials with a sum of degrees $< m + n$. We prove it for the sum equal to $m + n$. With regard to the symmetry we can suppose $m > n$. From the identity

$$(x^m - a) - x^{m-n}(x^n - b) = b\left(x^{m-n} - \frac{a}{b}\right)$$

follows

$$(x^m - a, x^n - b) = \left(x^{m-n} - \frac{a}{b},\ x^n - b\right). \tag{6}$$

It is $(m - n) + n = m < m + n$ and $(m - n, n) = (m, n) = d$. Using the supposition we get from (6) first that the degree of the left hand side in (6) is 0 or d. Secondly, the condition (5) for the right hand side of (6) has the form

$$\left(\frac{a}{b}\right)^{\frac{n}{d}} = b^{\frac{m-n}{d}}.$$

But this equation is equivalent to (5) and now (6) gives us the proof.

No we prove the theorem of SCHWARZ.

Let σ_k denote the number of irreducible factors of degree k of the polynomial (1). It is well-known that

$$(x^m - a, x^{P^k-1} - 1) \tag{7}$$

is the product of all irreducible factors of (1) whose degrees are divisors of k. Since $p \nmid m$, the polynomial (1) has no mutiple factors and we have

$$\sum_{t/k} t\sigma_t = \text{degree of (7)}. \tag{8}$$

According to the Lemma proved above the degree of (7) is 0 or $d_k = (m, P^k - 1)$. The second case occurs if and only if

$$a^{d'_k} = 1 \quad \left(d'_k = \frac{P^k - 1}{d_k}\right) \tag{9}$$

holds. Therefore if $\varkappa_k$ denotes the characteristic function of the statement (9) (i. e. 1 or 0 according as (9) holds or not) the degree of (7) has the form $d_k\varkappa_k$. Using the MÖBIUS formula for inversion we get from (8)

$$k\sigma_k = \sum_{t/k} \mu\left(\frac{k}{t}\right) d_t\varkappa_t.$$

This is equivalent to (2) and the Theorem is proved.

Krátký důkaz jedné věty Št. Schwarze o konečných tělesech.

(Obsah předešlého článku.)

Jde o důkaz věty z článku SCHWARZOVA, uvedeného v poznámce [1] pod čarou.