Časopis pro pěstování matematiky a fysiky

Štefan Schwarz

On universal forms in finite fields

Časopis pro pěstování matematiky a fysiky, Vol. 75 (1950), No. 2, 45--50

Persistent URL: http://dml.cz/dmlcz/120770

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

ON UNIVERSAL FORMS IN FINITE FIELDS.

ŠTEFAN SCHWARZ, Bratislava.

(Received January 17, 1949.)

In two recent papers[1]) I dealt with the representation of the elements of a finite field $GF(p^n)$ by the forms

$$x_1^k + x_2^k + \ldots + x_k^k \tag{1}$$

and

$$a_1x_1^k + a_2x_2^k + \ldots + a_kx_k^k, \quad a_i \in GF(p^n), \quad a_1a_2 \ldots a_k \neq 0. \tag{2}$$

I proved that these forms are universal[2])

α) for the form (1), if we suppose

$$(p^n - 1, k) \leqq p - 1,$$

β) for the form (2), if we make the stronger supposition $k \mid p - 1$.

The proof of the first statement was based upon an induction; the proof of the second on a method originally due to V. A. LEBESGUE and generalised by several authors.

The purpose of this paper is to show

i) the form (2) is universal even, if we suppose only $(p^n - 1, k) \leqq \leqq p - 1$,

ii) the proof of this fact (which cannot be proved by means of the LEBESGUE method[3])) can be given by a not too complicated induction in an analogous way as that for the form (1).

We prove the following theorem.

Theorem. *Suppose that* (*i*) $GF(p^n)$ *is a finite field of characteristic* p. (*ii*) $a_1, a_2, \ldots, a_k$ *are elements of the field* $GF(p^n)$, $a_1a_2 \ldots a_k \neq 0$. (*iii*) $\delta =$

---

[1]) „On WARING'S problem in finite fields", Quart. J. of Math. (Oxford), **19** (1948), 123—128; „On the equation $a_1x_1^k + a_2x_2^k + \ldots + a_kx_k^k + b = 0$ in finite fields", ibidem **19** (1948), 160—163.

[2]) That is: every $b \in GF(p^n)$ can be represented by the form (1) or (2) respectively with $x_1, x_2, \ldots, x_k \in GF(p^n)$.

[3]) See the footnote l. c.[1]), p. 162.

$= (p^n - 1, k) \leqq p - 1$. *Then the equation*

$$b = a_1x_1^k + a_2x_2^k + \ldots + a_kx_k^k$$

has a solution with $x_1, x_2, \ldots, x_k \in GF(p^n)$ *for every* $b \in GF(p^n)$.

To simplify the proof we divide it in five parts.

1. Trivial cases. The only substantial case is $(p^n - 1, k) = k$. I treat first the cases $(p^n - 1, k) = 1$ and $1 < \delta = (p^n - 1, k) < k$.

α) Let $(p^n - 1, k) = 1$. Then it is well-known that if x_1 runs through all elements of $GF(p^n)$ the expression x_1^k and the expression $a_1x_1^k$ take all values of $GF(p^n)$. There exist therefore to every element $b \in GF(p^n)$ such elements

$$\xi_1 \neq 0,\ \xi_2 = \xi_3 = \ldots = \xi_k = 0,\ \xi_1 \in GF(p^n)$$

that the relation

$$b = a_1\xi_1^k + a_2 \,.\, 0^k + \ldots + a_k \,.\, 0^k$$

holds.

β) Let $1 < \delta = (p^n - 1, k) < k$. Then there exist two integers x, y with $x(p^n - 1) + y \,.\, k = \delta$. Hence

$$\xi^\delta = \xi^{x(p^n-1)+yk} = (\xi^y)^k$$

for every $\xi \in GF(p^n)$. Every δ-th power is at the same time a k-th power. We have now $(p^n - 1, \delta) = \delta$. If we suppose the theorem proved in the case $(p^n - 1, k) = k$, then every $b \in GF(p^n)$ is representable by means of the form

$$a_1x_1^\delta + \ldots + a_\delta x_\delta^\delta,\ a_1a_2 \ldots a_\delta \neq 0.$$

There exist therefore elements $\xi_1, \xi_2, \ldots, \xi_\delta \in GF(p^n)$ such that

$$b = a_1\xi_1^\delta + a_2\xi_2^\delta + \ldots + a_\delta\xi_\delta^\delta.$$

Thus, we can write

$$b = a_1(\xi_1^y)^k + a_2(\xi_2^y)^k + \ldots + a_\delta(\xi_\delta^y)^k + a_{\delta+1} \,.\, 0^k + \ldots + a_k \,.\, 0^k,$$

q. e. d.

In what follows we can and shall suppose therefore allways $k \mid p^n-1$.

2. Construction of a special field $GF(p^n)$. Let T_p be the field of all residue-classes modulo p. Without fear of misunderstanding we shall denote the elements of T_p by the integers $0, 1, 2, \ldots, p - 1$. The field $GF(p^n)$ is obtained from the field T_p by adjunction of a root j of an irreducible equation $f(x) = 0$ of degree n. Every element of the field $T_p(j) = GF(p^n)$ is of the form

$$\xi = u_0 + u_1j + \ldots + u_{n-1}j^{n-1},\ u_i \in T_p.$$

We can formally realize the field $T_p(j) = GF(p^n)$ in several ways according to the choice of the irreducible polynomial $f(x)$ the root j of which we use in constructing the field $T_p(j)$. But it is well-known that two such fields (defined for the same n) are isomorphic with respect to T_p. Therefore it is sufficient to prove our theorem for a special field of this type.[4])

Let us now take for the irreducible polynominal $f(x)$ by means of whose root we realize the field $GF(p^n)$ such an irreducible polynomial of the field T_p of degree n which divides

$$x^{\frac{p^n-1}{k}}-1.$$

The existence of such a polynomial is assured by the following Lemma:

Lemma: *Let n, k be two integers such that*

$$n \geqq 1,\ k \mid p^n - 1,\ 1 < k \leqq p - 1.$$

Then there exist in T_p an irreducible polynomial of degree n which divides

---

[4]) The explicit proof of this statement is as follows.

Let us suppose that our theorem holds for the field $T_p(j)$ generated by the root j of the irreducible equation $\epsilon\, T_p$ $f(x) = 0$. That is, let us suppose that every form $a_1x_1^k + a_2x_2^k + \ldots + a_kx_k^k$, $a_1, a_2, \ldots, a_k \in T_p(j)$, is universal in $T_p(j)$.

Let be $T_p(j^*)$ the field generated by a root j^* of an other irreducible polynomial $f^*(x) \in T_p$ of degree n. We have to show that every form

$$a_1^*x_1^k + a_2^*x_2^k + \ldots + a_k^*x_k^k, \tag{A}$$

$a_1^*, a_2^*, \ldots, a_k^* \in T_p(j^*)$, is universal in $T_p(j^*)$. We prove that the equation

$$b^* = a_1^*x_1^k + a_2^*x_2^k + \ldots + a_k^*x_k^k \tag{B}$$

has for every $b^* \in T_p(j^*)$ at least one solution with $x_1, x_2, \ldots, x_k \in T_p(j^*)$.

It is well-known that the numbers j, j^* depend one on another rationally. That is, two relations of the form $j = \varphi(j^*)$, $j^* = \psi(j)$ hold, where $\varphi(z)$ and $\psi(z)$ are polynomials in z (with coefficients in T_p) of degree at most $n - 1$.

The transformation

$$j^* \to \psi(j) \tag{C}$$

is a one to one mapping of the field $T_p(j^*)$ into the field $T_p(j)$. The mapping (C) carries the form (A) into the form $a_1x_1^k + \ldots + a_kx_k^k$, $a_1, a_2, \ldots, a_k \in T_p(j)$. The number $b^* \in T_p(j^*)$ is carried into the number $b \in T_p(j)$.

Consider now the equation in $T_p(j)$

$$b = a_1x_1^k + a_2x_2^k + \ldots + a_kx_k^k.$$

According to the supposition this equation has at least one solution. There exist therefore numbers $\xi_1, \xi_2, \ldots, \xi_k \in T_p(j)$ such that the relation

$$b = a_1\xi_1^k + a_2\xi_2^k + \ldots + a_k\xi_k^k \tag{D}$$

holds.

The inverse mapping $j \to \varphi(j^*)$ carries (D) into the true relation

$$b^* = a_1^* \cdot \xi_1^{*k} + a_2^* \cdot \xi_2^{*k} + \ldots + a_k^*\xi_k^{*k}$$

with $\xi_1^*, \xi_2^*, \ldots, \xi_k^* \in T_p(j^*)$. The equation (B) has in $T_p(j^*)$ a solution, q. e. d.

the polynomial

$$x^{(p^n-1)/k}-1. \tag{3}$$

The proof of this Lemma for $n > 1$ is given l. c.[1]) p. 124—125. (The case $n = 1$ is trivially true.)

The irreducible polynomial $f(x)$ divides (3). Thus, j satisfies the equation $j^{(p^n-1)/k} = 1$. The element j is a k-th power in $GF(p^n)$,[5]) that is, there exist a number $\xi_0 \in GF(p^n)$ such that $j = \xi_0{}^k$ holds.

This choice of the number j will very simplify our later investigations.

3. Futher notations. Let us denote by $\mathfrak{G}$ the multiplicative group of the field $GF(p^n)$, by $\mathfrak{H}$ the sub-group of k-th powers. The decomposition of $\mathfrak{G}$ modulo $\mathfrak{H}$ has the form[6])

$$\mathfrak{G} = d_1\mathfrak{H} + d_2\mathfrak{H} + \ldots + d_k\mathfrak{H} \tag{4}$$

$[d_i \in GF(p^n)$, one of the d_i is equal to 1 (unity element)].

In what follows I call the numbers $u_0, u_1, \ldots, u_{n-1} \in T_p$ the *coordinates* of the element

$$d = u_0 + u_1 j + \ldots + u_{n-1} j^{n-1}$$

and the number of coordinates different from zero the *length* of the element d. The length l is an integer, $1 \leqq l \leqq n$. The following remark is of great importance: If a co-set $d_i\mathfrak{H}$ contains an element d of the length l, then there exist in $d_i\mathfrak{H}$ an element of the same length l having the first coordinate u_0 different from zero. For, if the number

$$u_\rho j^\rho + u_{\rho+1} j^{\rho+1} + \ldots + u_{n-1} j^{n-1} \quad (u_\rho \neq 0,\ \varrho \geqq 1)$$

belongs to $d_i\mathfrak{H}$, so does the number

$$j^{-\rho}[u_\rho j^\rho + \ldots + u_{n-1} j^{n-1}] = u_\rho + u_{\rho+1} j + \ldots + u_{n-1} j^{n-\rho-1}$$

(since $j^{-\rho}$, being a k-th power, belongs to $\mathfrak{H}$).

4. The arrangement of the co-sets of $\mathfrak{H}$. Now we choose the arrangement of the co-sets of $\mathfrak{H}$ in (4) in a special way.

First take the co-set $a_1\mathfrak{H}$. Then take the co-set $c_2(a_2\mathfrak{H})$, where c_2 is chosen as follows. Among all numbers c_2 satisfying the condition

$$c_2(a_2\mathfrak{H}) \subset \mathfrak{G} - a_1\mathfrak{H}$$

we take those with the smallest length l_2. From them we choose the

[5]) The multiplicative group of the field $GF(p^n)$ is cyclic. See van der Waerden, Moderne Algebra I. Teil, 2. Auflage, p. 123. Therefore every element satisfying the equation $x^{(p^n-1)/k} = 1$ is a k-th power.

[6]) The group $\mathfrak{G}$ being cyclic, the subgroup of the k-th powers has under $\mathfrak{G}$ the index k.

element

$$c_2 = c_{02} + c_{12}j + \dots + c_{n-1,2}j^{n-1}$$

such that $c_{02} \neq 0$ and, moreover, c_{02} has the least possible positive value $\geqq 1$. According to the remark at the end of section 3 such an element allways exists.

Then take the coset $c_3(a_3\mathfrak{H})$, where c_3 is chosen again as follows. Among all numbers c_3 satisfying the condition

$$c_3(a_3\mathfrak{H}) \subset \mathfrak{G} - a_1\mathfrak{H} - c_2(a_2\mathfrak{H})$$

we take those with the smallest length l_3. From them we choose the element

$$c_3 = c_{03} + c_{13}j + \dots + c_{n-1,3}j^{n-1}$$

such that $c_{03} \neq 0$ and c_{03} has again the least possible positive value $\geqq 1$.

We repeat this process just k times.

The last element

$$c_k = c_{0k} + c_{1k}j + \dots + c_{n-1,k}j^{n-1}$$

will be chosen as follows. We find first all numbers c_k of the least possible length having the property

$$c_k(a_k\mathfrak{H}) \subset \mathfrak{G} - a_1\mathfrak{H} - c_2(a_2\mathfrak{H}) - \dots - c_{k-1}(a_{k-1}\mathfrak{H}).$$

Then among them we choose an element whose first coordinate c_{0k} has the least possible positive value $\geqq 1$.[7])

The rearrangement of the decomposition (4) has the final form

$$\mathfrak{G} = a_1\mathfrak{H} + c_2(a_2\mathfrak{H}) + c_3(a_3\mathfrak{H}) + \dots + c_k(a_k\mathfrak{H}).$$

5. The main part of the proof. To show now that every element $\epsilon GF(p^n)$ is representable by the form (2) it is sufficient to prove that each of the elements

$$a_1c_1,\ a_2c_2,\ a_3c_3,\ \dots,\ a_kc_k \quad (c_1 = 1)$$

can be written in the form (2).

This will be proved, if we show that every a_ic_i $(1 \leqq i \leqq k)$ can be already written in the form

$$a_ic_i = a_1\xi_1^k + a_2\xi_2^k + \dots + a_i\xi_i^k$$

with $\xi_1, \xi_2, \dots, \xi_i \in GF(p^n)$.

The proof follows by induction.

The statement is true for $i = 1$, since $a_1c_1 = a_1 = a_1 \,.\, 1^k$. Now supposing our statement true for all a_tc_t with $1 \leqq t < i$ we prove it for a_ic_i.

Let be

$$c_i = c_{0i} + c_{1i}j + \dots + c_{n-1,i}j^{n-1}.$$

7) Such a number c_k allways exists since there are exactly k co-sets in the decomposition (4).

Let its length be l_i. We form the co-set $(c_i - 1) \,.\, a_i\mathfrak{H}$. Let us consider the number

$$c_i - 1 = (c_{0i} - 1) + c_{1i}j + \ldots + c_{n-1,i}j^{n-1}.$$

If $c_{0i} = 1$, $c_i - 1$ has a length less than c_i. If $c_{0i} \neq 1$, $c_i - 1$ has the length l_i but its first coordinate is less than that of the number c_i. In both cases — with respect to the definition of the number c_i — the co-set $(c_i - 1)\, a_i\mathfrak{H}$ does not belong to the set

$$\mathfrak{G} - a_1\mathfrak{H} - c_2(a_2\mathfrak{H}) - \ldots - c_{i-1}(a_{i-1}\mathfrak{H}).$$

It holds therefore

$$(c_i - 1)\, a_i\mathfrak{H} \subset c_1(a_1\mathfrak{H}) + c_2(a_2\mathfrak{H}) + \ldots + c_{i-1}(a_{i-1}\mathfrak{H}).$$

That means: there exists an index $t \leqq i - 1$ and a number ξ_0 such that

$$(c_i - 1)\, a_i = c_t a_t \,.\, \xi_0{}^k.$$

By the inductive supposition $c_t \,.\, a_t$ can be written in the form

$$c_t a_t = a_1\xi_1{}^k + a_2\xi_2{}^k + \ldots + a_{i-1}\xi_{i-1}{}^k.$$

Therefore

$$c_i a_i - a_i = (a_1\xi_1{}^k + \ldots + a_{i-1}\xi_{i-1}{}^k) \,.\, \xi_0{}^k,$$

$$c_i a_i = a_1(\xi_1\xi_0)^k + a_2(\xi_0\xi_2)^k + \ldots + a_{i-1}(\xi_{i-1}\xi_0)^k + a_i \,.\, 1^k,$$

which completes the proof.

O univerzálnych formách v konečných telesiach.

(Obsah predošlého článku.)

Obsahom predloženej práce je dőkaz tejto vety:

Nech $GF(p^n)$ je konečné teleso charakteristiky p. Nech $a_1, a_2, \ldots, a_k$ sú elementy telesa $GF(p^n)$, $a_1 \,.\, a_2 \ldots a_k \neq 0$. Nech k je celé číslo $\geqq 1$, $\delta = (p^n - 1, k) \leqq p - 1$. Potom každé číslo b telesa $GF(p^n)$ dá sa písať v tvare

$$b = a_1x_1{}^k + a_2x_2{}^k + \ldots + a_kx_k{}^k,$$

kde $x_1, x_2, \ldots, x_k$ sú vhodne volené prvky z telesa $GF(p^n)$.