RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

ENDRINA BERMUDEZ
MARISELA MAYZ
OFELIA PEROTTI

A geometric characterization of the generators in an extension of odd prime order of a finite field

Rendiconti del Seminario Matematico della Università di Padova, tome 74 (1985), p. 15-22

<http://www.numdam.org/item?id=RSMUP_1985__74__15_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 74 (1985)

A Geometric Characterization of the Generators in an Extension of Odd Prime Order of a Finite Field.

ENDRINA BERMUDEZ - MARISELA MAYZ - OFELIA PEROTTI (*)

SUMMARY - In this paper we generalize some properties found in [1] to the case of extensions of odd prime order of a finite field.

1. Introduction.

Let p and r be odd primes. We consider a finite field $K = GF(q)$ with $q = p^n$ elements and an extension K' of K of order r. We denote by K^* and K'^* the multiplicative cyclic groups of non-zero elements of K and K', respectively, and by Λ and Λ' the sets of all generators of K^* and K'^*.

In this paper we consistently use b and h to denote the following numbers:

$$b = q-1, \qquad h = \frac{q^r-1}{q-1}$$

$$\left(= b^{r-1} + \binom{r}{1} b^{r-2} + \ldots + \binom{r}{r-2} b + r = h_1 b + r\right).$$

Thus, K^* has b elements and $\varphi(b)$ generators (where φ denotes the Euler function), while K'^* has hb elements and $\varphi(hb)$ generators.

We observe that a common divisor of h and b must divide the prime r.

(*) Indirizzo degli AA.: Universidad Simän Bolívar, Sartenejas, Caracas, Venezuela.

Hence:

i) if r does not divide b, then $(b, h) = 1$ and $\varphi(bh) = \varphi(b)\varphi(h)$, while

ii) if r divides b, then

$$(b, h) = r \quad \text{and} \quad \varphi(bh) = \frac{r}{r-1}\varphi(b)\varphi(h) .$$

We will also consider the multiplicative group homomorphism defined by the « norm »:

$$N: K'^* \to K^* , \quad N(q) = q^h .$$

It is well known that N is surjective (and one may prove it by observing that the norm of a generator of K'^* must be a generator of K^*, so that the image of N contains K^*).

2. Geometric properties of Λ'.

It is convenient to think of K' as the r-dimensional affine space K^r over K.

In this paper we will be interested in the following types of subsets:

i) lines through the origin;

ii) hypersurfaces of constant norm.

A line through the origin will be represented, in parametric form, by:

$$\begin{cases} \xi = t\lambda \\ t \in K , \quad \text{with fixed nonzero } \lambda \in K' . \end{cases}$$

We will (improperly, if $r > 3$) call a « surface of constant norm » every subset, C_n, of K' formed by all the elements of K' whose norm is n $(\in K^*)$.

As N is an epimorphism, every surface of constant norm will have exactly h elements. It is also evident that every line, $L(\lambda)$, passing through the origin and the non-zero element λ, has exactly q elements.

We will call a «generator line» any line through the origin, which contains at least one generator of K'^*. We will call a «primitive surface» each surface of constant norm, C_n, whose norm n is a generator of K^*.

PROPOSITION 1. Every element of each generator line has order (in the multiplicative group K'^*) hb/d equal to the order of its norm, multiplied by h. (The number d is a divisor of b which is not a multiple of r.)

PROOF. If we consider a line through the origin containing the generator λ of norm g, then every nonzero element of this line may be expressed in the form:

$$g^k \lambda , \quad 0 < k \leqslant b ,$$

and also in the form: λ^{hk+1} (because $\lambda^h = g$).

The order of $g^k \lambda$ is:

$$O(g^k \lambda) = \frac{hb}{(hb, hk + 1)} ,$$

and the order of its norm, g^{kr+1}, is:

$$O(g^{kr+1}) = \frac{b}{(b, kr + 1)} .$$

Therefore, if we observe that: $(hb, hk + 1) = (b, hk + 1) = (b, rk + 1)$, we see that:

$$O(g^k \lambda) = h \cdot O(N(g^k \lambda)) .$$

Putting $d = (b, rk + 1)$ we also have that d divides b and that r does not divide d.

COROLLARY 1.1. Given any number d (of the form $d = (rk + 1, b)$ in order to avoid trivial cases) all generator lines have the same number of elements of order hb/d.

This follows by observing that the number $(rk + 1, b)$ does not depend on the generator β which determines the generator line.

OBSERVATION. In propositions 2 and 3 we will determine the exact number of elements of order hb/d contained in any generator line.

COROLLARY 1.2. The set Λ', of all generators of K'^* is the intersection, R, of the union of all generator lines with the union of all primitive surfaces.

In effect $\Lambda' \subseteq R$, since every generator of K'^* belongs to some generator line and has norm which is a generator of K^*; conversely, every element $t \in R$ is an element of some generator line, whose order is hb/d and whose norm has order $b/d = b$; therefore $d = 1$ and t is a generator of K'^*.

PROPOSITION 2. If r does not divide b, then:

i) K'^* is the direct product of its subgroups C_1 and K^*; that is, every element of K'^* may be expressed, in an unique way, as a product of an element of norm 1 by its norm.

ii) Every surface C_n intersects each line through the origin in exactly one point.

iii) On every generator line there are exactly $\varphi(b/d)$ elements of order hb/d (for every number d which divides b); in particular, there are $\varphi(b)$ generators on every generator line.

iv) There are $\varphi(h)$ generator lines.

v) On every primitive surface there are $\varphi(h)$ generators.

PROOF.

i) This follows immediately by observing that C_1 has h elements, K^* has b elements, and $(h, b) = 1$.

ii) Observing that $a^r = c^r$ implies $a = c$ for any $a, c \in K$ (since r does not divide b), we have that the elements of a line through the origin have distinct norms.

iii) Since every element of a fixed line through the origin is determined by its norm and since the order of every element of this line is equal to the product of the order of its norm by h (see proposition 1), we have that the number of elements of order hb/d of any generator line will be equal to the number of elements of K^* whose order is b/d, that is $\varphi(b/d)$.

iv) If M is the number of generator lines, then observing that each generator line has $\varphi(b)$ generators and remembering from section 1 that K'^* has $\varphi(h)\varphi(b)$ generators, one must have $M \cdot \varphi(b) = \varphi(h) \cdot \varphi(b)$, and therefore $M = \varphi(h)$.

v) Any element of a primitive surface is a generator of K'^*, if and only if it belongs to some generator line (corollary 1.2). Therefore, by ii) and iv) the number of generators on a primitive surface will be $\varphi(h)$.

PROPOSITION 3. Let r divide b.

Let $R_0, R_1, \ldots, R_{r-1}$ (respectively $R'_0, R'_1, \ldots, R'_{r-1}$) be the cosets of K^* (respectively K'^*) corresponding to the subgroup R_0 (respectively R'_0) of the r-th powers of elements of K^* (respectively K'^*).

For a fixed generator, ξ, of K'^* we will denote by R'_i the coset of K'^* which contains ξ^i and by R_i the coset of K^* which contains m^i, where m is the norm of ξ and $i = 0, 1, \ldots, r-1$.

Then we have:

i) The intersection of any surface C_n with any line through the origin contains exactly r points or is empty.

ii) R'_i is the union of all C_n surfaces whose norm n belongs to R_i; R'_i is also the union of lines through the origin.

iii) All R'_i distinct from R'_0 contain the same number, $\varphi(b)/(r-1)$, of primitive surfaces.

iv) On every generator line there are exactly $(r/(r-1))\varphi(b/d)$ elements of order hb/d, for every d which divides b but is not divisible by r; in particular there are exactly, $(r/(r-1))\varphi(b)$ generators on every generator line.

v) There are $\varphi(h)$ generator lines.

vi) All R'_i distinct from R'_0 contain the same number, $\varphi(h)/(r-1)$, of generator lines.

vii) On every primitive surface there are exactly $(r/(r-1))\varphi(h)$ generators.

PROOF.

i) If the intersection $L(\lambda) \cap C_n$ is not empty, let $a\lambda, a'\lambda$ be two elements of this intersection. Since they have the same norm, one must have $N(a\lambda) = N(a'\lambda)$, $N(a) = N(a')$ and

$a^r = a'^r$; therefore $a' = a \cdot g^{(ib/r)}$, with g a generator of K^* and $i = 1, 2, \ldots, r$.

ii) Observe that an element λ belongs to R_i' if and only if $\lambda = \xi^t$, with $(t - i)$ divisible by r, that is, if and only if $N(\lambda) \in R_i$. We observe also that if $\lambda \in R_i'$, then for all $a \in K^*$ we have $a = m^s = \xi^{hs}$ with convenient s, and therefore $a\lambda = \xi^{n+hs}$ and, as r divides h, we have also that $(n + hs - i)$ is divisible by r if and only if $(n - i)$ is divisible by r.

iii) This follows from lemma 2 in section 3 (appendix), which states that the same number of generators of K^* are found in each coset R_i distinct from R_0.

iv) Let d be a divisor of b which is not a multiple of r and let M be the number of elements of order hb/d on the line $L(\lambda)$ determined by the generator λ with norm g.

We obtain all nonzero elements of this line, by the expressions

$$g^k\lambda, \quad k = 0, 1, 2, \ldots, b - 1 .$$

Observing that the order of $g^k\lambda$ is $hb/(b, rk + 1)$, we must determine for how many values of k (in the interval $[0, b - 1]$) one has that $(b, rk + 1) = d$. As r and d are relatively prime (and, moreover, d divides b), in the arithmetic progression of b terms and difference r:

$$1, \ 1 + r, \ 1 + 2r, \ \ldots, \ 1 + (b - 1)r$$

there will be b/d terms which are divisible by d. If we then indicate by $a_0 d$ the first of them, M will also be the number of terms $a_0 d + i\,dr$ such that $(a_0 d + i\,dr, b) = d$, in the sub-progression:

$$a_0 d, \ a_0 d + dr, \ \ldots, \ a_0 d + idr, \ \ldots, \ a_0 d + \left(\frac{b}{d} - 1\right) dr$$

that we obtain eliminating all terms which are not divisible by d.

Also M will be the number of terms of the new progression:

$$a_0, \ a_0 + r, \ \ldots, \ a_0 + \left(\frac{b}{d} - 1\right) r$$

which are relatively prime with b/d.

Therefore, by lemma 1 (see section 3) we have:

$$M = \frac{r}{r-1}\varphi\left(\frac{b}{d}\right).$$

v) As the number of generators of K'^* is $(r/(r-1))\varphi(h)\varphi(b)$ (see section 1), and since there are $(r/(r-1))\varphi(b)$ generators on every generator line, one has that if R is the number of generator lines, then

$$\frac{r}{r-1}\varphi(h)\varphi(b) = R\frac{r}{r-1}\varphi(b), \qquad \text{and therefore} \qquad R = \varphi(h).$$

vi) By lemma 2 (see section 3) applied to the group K'^* we have that there are

$$\frac{\varphi(bh)}{r-1} = \frac{r}{(r-1)^2}\varphi(h)\varphi(b),$$

generators in each coset R_i' distinct from R_0', and, as every generator line has $(r/(r-1))\varphi(b)$ generators, there will be $\varphi(h)/(r-1)$ generator lines in each coset.

vii) One verifies this with the same argument as vi), observing that there are $\varphi(b)/(r-1)$ primitive surfaces in each coset.

3. Appendix.

LEMMA 1. Let N be any natural number, r a prime factor of N and m a natural number not divisible by r. Then there are exactly $\varphi(N)/(r-1)$ terms which are relatively prime with N in the arithmetic progression of N terms:

$$m,\ m+r,\ \ldots,\ m+(N-1)r.$$

LEMMA 2 (COROLLARY OF LEMMA 1). Let G be a cyclic group of N elements and r a proper prime divisor of N; let G_0 be the subgroup (of index r) of all r-th powers of elements of G and let $G_1, \ldots, G_{r-1}$ be the other cosets. Then in each coset, distinct from G_0, there is the same number $\varphi(N)/(r-1)$ of generators of G.

PROOF OF LEMMA 1. We may obtain the formula by observing that if $r, t_1, \ldots, t_n$ are all different prime factors of N, then there will be $(1-1/t_1)N$ terms in the progression which are not divisible by t_1, and of these $(1-1/t_1)(1-1/t_2)N$ will not be divisible by t_2, and so on. In this way we find $N \cdot \prod_{i=1}^{n} (1-1/t_i)$ terms which are relatively prime with N, and the formula follows by remembering that $\varphi(N) = N(1-1/r)\prod_{i=1}^{n}(1-1/t_i)$.

PROOF OF LEMMA 2. Let g be a generator of G and let G_i be the coset which contains g^i (for all i such that $0 \leqslant i < r$). An element g^{i+kr} of the coset g_i will be a generator if and only if $(i + kr, N) = 1$. Therefore the number of generators in a certain coset will be the number of terms in the arithmetic progression of N/r terms and difference r:

$$i, i+r, \ldots, i+\left(\frac{N}{r}-1\right)r$$

which are relatively prime to N.

Observing that $g^{i+N} = g^i$, this number will also be equal to $1/r$ times the number of terms of the arithmetic progression of N terms and difference r:

$$i,\ i+r,\ \ldots,\ i+(N-1)r$$

which are relatively prime to N. Therefore by the lemma 1 we have:

$$\frac{1}{r}\,\frac{r}{r-1}\,\varphi(N) = \frac{\varphi(N)}{r-1}\,.$$

BIBLIOGRAPHY

R. GIUDICI - C. MARGAGLIO, *A geometric characterization of the generators in a quadratic extension of a finite field*, Rend. Sem. Mat. Univ. Padova, **62** (1980).

Manoscritto pervenuto in redazione il 3 febbraio 1984.