

RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

REINALDO E. GIUDICI

CLAUDIO MARGAGLIO

**A geometric characterization of the generators in
a quadratic extension of a finite field**

Rendiconti del Seminario Matematico della Università di Padova,
tome 62 (1980), p. 103-114

http://www.numdam.org/item?id=RSMUP_1980__62__103_0

© Rendiconti del Seminario Matematico della Università di Padova, 1980, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

A Geometric Characterization of the Generators in a Quadratic Extension of a Finite Field.

REINALDO E. GIUDICI - CLAUDIO MARGAGLIO (*)

SUMMARY - Let $K' = GF(p^{2n})$ be a quadratic extension of the Galois field $K = GF(p^n)$, where p is an odd prime. In this article we deal with a geometric characterization of the set of generators of the multiplicative cyclic group of K' in terms of a generator of the multiplicative cyclic group of K . With this characterization the set of generators of $(K')^* = K' - \{0\}$ is just the intersection of two sets which are respectively the union of sets of certain lines through the origin and « conics with primitive norm ». As an application of the idea developed in this article we prove that for some special primes, like Fermat's primes, there exists a generator of $GF^*(p^2)$ with any one of its coordinates ($\neq 0$) preassigned. It is also proved that the first component of a generator can be assigned $= 1$ for primes p such that $p \equiv 1 \pmod{4}$ and $p < (3.5) \cdot 10^{15}$. At the same time we provide an alternative method for computing all of the generators of the quadratic extension $GF^*(p^{2n})$.

1. Introduction.

We consider a finite field, K , with $q = p^n$ elements, p odd prime. If g is a generator of the multiplicative cyclic group $K^* = K - \{0\}$,

(*) Indirizzo degli AA.: Department of Mathematics, Universidad Simon Bolivar - Caracas (Venezuela).

we consider the quadratic extension K' of K by $X^2 - g$, so that

$$(1.1) \quad K' = \{a + b\theta \mid a, b \in K\}, \quad \theta^2 = g \quad (\theta \text{ fixed}).$$

We denote by $\mathcal{A}$ the set of all generators of K^* and by $\mathcal{A}'$ the set of all generators of the multiplicative cyclic group $(K')^* = K' - \{0\}$.

Since K^* has $q - 1$ elements and $(K')^*$ has $q^2 - 1$ elements, $\mathcal{A}$, $\mathcal{A}'$ will be, respectively, sets of $\varphi(q - 1)$, $\varphi(q^2 - 1) = 2\varphi(q - 1)\varphi(q + 1)$ elements where φ represents the « Euler function ».

It will also be useful to consider the norm homomorphism,

$$N: (K')^* \rightarrow K^*$$

defined by

$$(1.2) \quad N(a + b\theta) = (a + b\theta)^{q+1} = a^2 - b^2g,$$

which is onto and partitions $(K')^*$ into $q - 1$ equivalence classes, each containing $q + 1$ elements of equal norm.

In particular, the norm of any generator λ of $(K')^*$ is a generator of K^* . That is,

$$(1.3) \quad N(\lambda) = \lambda^{q+1} = g^s, \quad \text{with } (s, q - 1) = 1.$$

This may be very useful for finding generators of $(K')^*$ and in two particular cases it is sufficient to determine them:

i) When $q = p = 2^m - 1$ is a Mersenne prime, we have $q + 1 = 2^m$ elements in $(K')^*$ with equal norm, and since there are $\varphi(q - 1)$ generators in K^* , we find $2^m\varphi(q - 1)$ elements of $(K')^*$ whose norm is a generator of K^* . Among these elements we must find all of the generators of $(K')^*$. But since $(K')^*$ has $2\varphi(q + 1)\varphi(q - 1) = 2^m\varphi(q - 1)$ generators, the elements whose norm is a generator of K^* are just all of the generators of $(K')^*$.

ii) When $q = p^n = 2p' - 1$ (p' and odd prime) there are $q + 1 = 2p'$ elements having norm a generator g' of K^* , but two of them are of the form $\pm b\theta$, because in this case $q \equiv 1 \pmod{4}$, and therefore -1 is a square in K and there is an element $b \in K$ such that $gb^2 = g'$. Hence, the elements $a + b\theta$ of $(K')^*$ having norm a generator of K^* and $a \neq 0$ are just all of the generators of $(K')^*$. This criterion is applied in several cases; for instance, if $q = 5, 13, 25$, etc.

2. Geometric properties of A' .

We identify the field K' , defined in (1.1) with the cartesian product $K \times K$ by associating the ordered pair (a, b) with $a + b\theta$ and we think of it as the affine plane $A^2(K)$ over K .

In this plane, we consider two distinguished types of subsets:

- i) « lines through the origin » and
- ii) « conics of constant norm ».

If $\xi = a + b\theta$ is any element of K' (different from zero), we define the line through the origin that contains ξ by

$$(2.1) \quad L(\xi) = \{(x, y) \in A^2(K) | bx - ay = 0, (a, b) \neq (0, 0)\},$$

and if h is any non-zero element of K , we define the « conic of norm h » to be

$$(2.2) \quad C_h = \{(x, y) \in A^2(K) | x^2 - gy^2 = h, h \in K^*\}.$$

It is also convenient to define

$$(2.3) \quad L^*(\xi) = L(\xi) \cap (K')^*.$$

It is easy to verify that every line $L(\xi)$ contains exactly q points and, by again using the fact that the norm is a homomorphism of $(K')^*$ onto K^* , that every conic C_h has exactly $q + 1$ points.

Observe that whenever a conic C_h contains a generator $\lambda \in A'$, then the norm h is a generator of K^* . In this case we call C_h a « conic of primitive norm ». On the other hand, a line through the origin which contains a generator of $(K')^*$ will be called a « generator line ».

THEOREM 1. Every non-zero element of a generator line has order of the form $(q^2 - 1)/d$, with d an odd divisor of $q - 1$, and for every odd divisor d of $q - 1$, there are exactly $2\varphi((q - 1)/d)$ elements in each generator line having order $(q^2 - 1)/d$.

PROOF: Let λ be any generator of $(K')^*$, $L(\lambda)$ the generator line which contains λ , and α any element of $L^*(\lambda)$. Then $\alpha = h\lambda$, $h \in K^*$,

and if $g_1 = \lambda^{q+1}$ is the norm of λ , we may write

$$(2.4) \quad h = g_1^k = \lambda^{k(q+1)},$$

$$(2.5) \quad \alpha = h \cdot \lambda = \lambda^{k(q+1)+1},$$

with a convenient exponent $k \in [0, q-2]$.

Then, the order of α in the cyclic group $(K')^*$ of order $q^2 - 1$ will be

$$O(\alpha) = \frac{q^2 - 1}{(k(q+1) + 1, q^2 - 1)} = \frac{q^2 - 1}{(2k + 1, q - 1)},$$

because

$$\begin{aligned} (k(q+1) + 1, q^2 - 1) &= (k(q+1) + 1, q - 1) = \\ &= (k(q-1) + 2k + 1, q - 1) = (2k + 1, q - 1). \end{aligned}$$

In this way we have that every element of $L^*(\lambda)$ has order of the form $(q^2 - 1)/d$, where $d = (2k + 1, q - 1)$ is an odd divisor of $q - 1$.

To count the number of elements of order $(q^2 - 1)/d$ contained in $L^*(\lambda)$, with fixed d , observe that we obtain all elements of $L^*(\lambda)$ by using the formula $\alpha = g_1^k \cdot \lambda$, where k takes on all values in the interval of integers $[0, q-2]$, or equivalently where $2k + 1$ takes on all odd values in the interval of integers $[1, 2q-2]$. Now, $g_1^k \cdot \lambda$ will have order $(q^2 - 1)/d$ if and only if $(2k + 1, q - 1) = d$ and this takes place $\varphi((q-1)/d)$ times when $2k + 1$ is in $[1, q-1]$ and the same number of times when $2k + 1$ is in $[q, 2(q-1)]$ because $d, 2k + 1$ are odd numbers and $q - 1$ is even, and if $s \in [q, 2(q-1)]$ then $(s, q - 1) = (s - (q - 1), q - 1)$ and $1 \leq s - (q - 1) \leq q - 1$.

Therefore, there are $2\varphi((q-1)/d)$ numbers of the form $2k + 1$ in $[1, 2(q-1)]$ such that $(2k + 1, q - 1) = d$, and we conclude that there are $2\varphi((q-1)/d)$ elements of order $(q^2 - 1)/d$ in our generator line $L^*(\lambda)$.

COROLLARY 1.1. There are $\varphi(q + 1)$ generator lines.

PROOF. Let M be the number of generator lines. There are $2\varphi(q-1)\varphi(q+1)$ generators of $(K')^*$ and each has order $q^2 - 1$.

Therefore, by Th. 1, there are $2\varphi(q-1)$ generators in each generator line, and since (by definition of generator line) every generator

belongs to some generator line, it follows that

$$(2.6) \quad 2\varphi(q-1)\varphi(q+1) = M2\varphi(q-1)$$

and therefore $M = \varphi(q+1)$.

COROLLARY 1.2. An element $\xi \in (K')^*$ belongs to some generator line if and only if its order is of the form

$$(2.7) \quad O(\xi) = \frac{q^2-1}{d}, \quad d \text{ an odd divisor of } q-1.$$

Moreover, if this holds, then

$$(2.8) \quad \frac{O(\xi)}{q+1} = O(N(\xi)),$$

so that an element ξ of a generator line is a generator of $(K')^*$ if and only if its norm is a generator of K^* .

PROOF. By Th. 1, every element of a generator line has order of the form $(q^2-1)/d$, with d an odd divisor of $q-1$. We must therefore verify that all elements of such order belong to some generator line.

Observe that there are in $(K')^*$, $\varphi((q^2-1)/d)$ elements of order $(q^2-1)/d$, with fixed d . Since both $q+1$, $(q-1)/d$ are even, we may write:

$$\varphi\left(\frac{q^2-1}{d}\right) = 2\varphi(q+1)\varphi\left(\frac{q-1}{d}\right)$$

and therefore, since $\varphi(q+1)$ is the number of generator lines (cor. 1.1) and $2\varphi((q-1)/d)$ is the number of elements of order $(q^2-1)/d$ in each generator line, we see that generator lines contain all such elements.

Finally we have

$$O(N(\xi)) = O(\xi^{q+1}) = \frac{O(\xi)}{(q+1, (q^2-1)/d)} = \frac{O(\xi)}{q+1}.$$

COROLLARY 1.3. A conic of constant norm h intersects generator lines if and only if h is not a square in K^* . Moreover, if h is not a

square in K^* the conic of norm h intersects each generator line in exactly two points that are elements of maximal order on the conic. In particular, if the norm of the conic is a generator of K^* then the conic intersects every generator line in two points that are generators of $(K')^*$.

PROOF. By cor. 1.2 all elements of a generator line have norms whose order is of the form

$$(2.9) \quad \frac{q^2 - 1}{d(q + 1)} = \frac{q - 1}{d} \quad (d \text{ an odd divisor of } q - 1),$$

and therefore, for any element ξ of a generator line, $N(\xi)$ is not a square in K^* . The above argument indicates that no conic of square-norm intersects generator lines. On the other hand, if a conic intersects a generator line it intersects it in exactly two points (which are opposite elements) and since there are $(q - 1)/2$ non-squares in K^* and every generator line has $q - 1$ points different from $(0, 0)$, it follows that all conics of non-square norm must intersect all generator lines.

Now, let h be a non-square of order $(q - 1)/d$ in K^* . Then every element ξ of norm h has order which divides $(q + 1)O(h)$, since $\xi^{(q+1)O(h)} = h^{O(h)} = 1$, and on the other hand, its intersections with a generator line are elements whose orders are $(q + 1)O(h)$, by cor. 1.2, which is the greatest possible.

COROLLARY 1.4. The set of generators of $(K')^*$ is just the intersection of the union of all generator lines with the union of all conics of primitive norm. In particular each conic of primitive norm contains $2\varphi(q + 1)$ generators and each generator line contains $2\varphi(q - 1)$ generators.

PROOF. By using cor. 1.2 or 1.3, any element of a generator line is a generator if and only if it has primitive norm and any element of a conic of primitive norm is a generator if and only if it belongs to some generator line. On the other hand every generator belongs to a generator line and to a conic of primitive norm.

Cor. 2.1 permits us to determine all generator lines in the following way: we take any non-square element h of K^* and search among the

elements of norm h for those that have maximal order ($q + 1$ times the order of h).

For instance, if $q \equiv 3 \pmod{4}$ we may take $h = -1$ and search for all elements of norm -1 having order $2(q + 1)$; if $q \equiv 1 \pmod{4}$, and if $q - 1 = 2^t m$ (m odd) we may search for all elements of norm g^m (g a generator of K^*) having order $2^t(q + 1)$.

Observe that the second case is the general one, since if $q \equiv 3 \pmod{4}$ then $q - 1 = 2^t m$ with $t = 1$ and $g^m = g^{(q-1)/2} = -1$.

In order to verify that an element λ of norm g^m has order $M = 2^t(q + 1)$, it is sufficient to check that $(\lambda)^{(M)/p_i} \neq 1$ for all different odd prime factors p_i of $q + 1$, since

$$(\lambda)^{2^{t-1}(q+1)} = (g^m)^{2^{t-1}} = g^{(q-1)/2} = -1.$$

The only cases in which it is not necessary to verify orders of elements are those mentioned at the end of section 1, that is, the cases when $q + 1 = 2^s$ or $q + 1 = 2p'$ (p' an odd prime).

3. An application to Giudici's conjecture.

R. Giudici made the following conjecture with respect to the generators of $(K')^* = GF^*(p^2)$, p an odd prime:

« For each $a \in K^* = GF^*(p)$ there exists at least one $\lambda \in A$ such that $\lambda = a + b\theta$ and for each $b \in GF^*(p)$ there exists at least one generator of $GF^*(p^2)$ of the form $a + b\theta$ ».

R. Frucht proved the validity of this conjecture for $a = 1$ and p a Fermat prime [1, thm. 6.1]. See also [2].

When p is a Fermat prime, one can also show that the number of generators with fixed a or fixed b is $\varphi(p + 1)$. However, this is not true for an arbitrary prime p . For instance, for $p = 23$ (not a Fermat prime) we obtain

$$n(1) = n(2) = n(5) = n(7) = n(8) = n(9) = n(10) = 4$$

and

$$n(3) = n(4) = n(6) = n(11) = 3$$

where we denote by $n(a)$ the number of generators of $GF^*(p^2)$ with given a .

For the known Fermat primes we have

p	3	5	17	257	65537
$\varphi(p+1)$	2	2	6	84	19800

We next establish a sufficient condition which $q = p^n$ may satisfy in order to comply with Giudici's conjecture in $K' = GF(p^{2^n})$.

THEOREM 2. If the number $q = p^n$ satisfies the inequality

$$(3.1) \quad \frac{1}{2}\varphi(q+1) + \varphi(q-1) > \frac{1}{2}(q-1)$$

then it also satisfies Giudici's conjecture in $GF^*(p^{2^n})$.

PROOF. It is evident that in each of the $\varphi(q+1)$ generator lines there is exactly one element with first (or second) component assigned. Now, by Cor. 1.3, the norm of any non-zero element of a generator line must be a non-quadratic residue in $GF^*(q)$.

Then, if for a first component a (or second b) there does not exist $\lambda \in A'$ such that $\lambda = a + b\theta$ then the $\varphi(q+1)/2$ different norms of the $\varphi(q+1)$ elements with fixed a (or b) belonging to the generator lines must be the elements of $(K')^*$ whose norm is neither a quadratic residue in K^* nor a generator of K^* .

Therefore, the number of such norms plus the number of primitive elements (generators) of K^* is less than or equal to the number of elements that are not quadratic residues in K^* ; that is,

$$\frac{1}{2}\varphi(q+1) + \varphi(q-1) \leq \frac{1}{2}(q-1).$$

It can easily be verified that a Fermat prime satisfies condition (3.1). There are 18 prime numbers less than 1000 that do not satisfy condition (3.1).

The 8 prime numbers less than 500 that do not satisfy condition (3.1) are: 139, 181, 211, 241, 331, 349, 379 and 421.

By direct verification, each of these satisfies Giudici's conjecture. Also primes of the form $p = 2p' + 1$, with p' an odd prime satisfy condition (3.1).

The following theorem gives a bound for primes of the form $4n+1$ that satisfy Giudici's conjecture when $a = 1$.

THEOREM 3. For each prime p such that $p \equiv 1 \pmod{4}$ and $p < (3, 5) \cdot 10^{15}$ there exists $\lambda \in A'$ of the form $\lambda = 1 + b\theta$.

PROOF. There are $p-1$ elements of the form $1 + b\theta$ with $b \neq 0$ in $GF^*(p^{2n})$. Let A be the set of elements of the form $1 + b\theta$ belonging to some generator line, i.e.

$$(3.2) \quad A = \{\lambda = 1 + b\theta \mid \lambda \in L^*(\lambda)\}.$$

Then, since the x and y axes (defined in an obvious way) are not generator lines we have $O(A) = \varphi(p+1)$.

Let $\bar{\Psi}$ be the number of generators g_i of $GF^*(p)$ such that $1 - g_i$ is not a quadratic residue in $GF^*(p)$. For each g_i there are two b such that $1 - g_i = gb^2$, that is, $N(1 + b\theta) = g_i$.

Let

$$(3.3) \quad B = \{1 + b\theta \mid N(1 + b\theta) \in A\}.$$

Then $O(B) = 2\bar{\Psi}$.

Following the argument of Jacobsthal [3, 239] we can prove that on every line parallel to the y -axis ($\neq y$ -axis) there are $(p-1)/2$ elements whose norm is a quadratic non-residue and since the elements of A and B lie between those elements we have $O(A \cup B) \leq (p-1)/2$.

Also, since

$$O(A \cap B) = O(A) + O(B) - O(A \cup B)$$

we have

$$(3.4) \quad O(A \cap B) \geq \varphi(p+1) + 2\bar{\Psi} - \frac{p-1}{2}.$$

Observe that the elements of $A \cap B$ are generators of $GF^*(p^{2n})$. Now let Ψ denote the character sum

$$(3.5) \quad \Psi = \sum_{g_i \in A} \chi(1 - g_i),$$

where A is the set of generators of $GF^*(p)$ and $\chi(1 - g_i)$ denotes the well known Legendre symbol $((1 - g_i)/p)$.

Let h be the number of g_i such that $\chi(1 - g_i) = 1$ and let k be the number of g_i with $\chi(1 - g_i) = -1$. We have

$$(3.6) \quad \begin{cases} h - k = \Psi, \\ h + k = \varphi(p-1). \end{cases}$$

Therefore,

$$(3.7) \quad \bar{\Psi} = k = \frac{1}{2}(\varphi(p-1) - \Psi).$$

Since $p \equiv 1 \pmod{4}$, $\chi(1) = \chi(-1)$, the inverse g_i^{-1} of any generator is a generator too, and

$$\Psi = \sum_{g_i \in A} \chi(1 - g_i) = \sum_{g_i \in A} \chi(g_i - 1) = - \sum_{g_i \in A} \chi(1 - g_i^{-1}) = -\Psi.$$

Thus, $\Psi = 0$ and by (3.7) $\Psi = k = \frac{1}{2}\varphi(p-1)$.

Thus, in (3.6) we have

$$(3.8) \quad 0(A \cap B) \geq \varphi(p+1) + \varphi(p-1) - \frac{1}{2}(p-1)$$

which represents a lower bound for the number of generators of the form $1 + b\theta$ with $p \equiv 1 \pmod{4}$.

We now prove that for $p \equiv 1 \pmod{4}$ and $p < (3.5) \cdot 10^{15}$ we have

$$(3.9) \quad \varphi(p+1) + \varphi(p-1) > \frac{1}{2}(p-1).$$

First of all, the only prime factor common to $p+1$ and $p-1$ is 2. Let us indicate by $q_1, q_2, \dots, q_t$ the distinct prime factors of p^2-1 that are different from 2 and by $d_1, d_2, \dots, d_t$ the numbers $d_i = (q_i-1)/q_i$.

Now, conveniently enumerating the q_i 's, we have

$$(3.10) \quad \frac{\varphi(p-1)}{p-1} = \frac{1}{2} d_1 d_2 \dots d_s,$$

$$(3.11) \quad \frac{\varphi(p+1)}{p+1} = \frac{1}{2} d_{s+1} d_{s+2} \dots d_t.$$

Since for Fermat primes we can verify directly the condition (3.1) and the Mersenne primes $2^n - 1$ are not congruent to 1 (mod 4) we can assume that both expressions (3.10) and (3.11) have at least one d_i occurring as a factor.

Let $d = \prod_{i=1}^t d_i$. We will first prove that if $d > \frac{1}{4}$ then

$$\frac{\varphi(p-1)}{p-1} + \frac{\varphi(p+1)}{p+1} > \frac{1}{2}.$$

Let $d = \frac{1}{4} + e$, $e > 0$, and consider the two products

$$(4.13) \quad \left\{ \begin{array}{l} U = \prod_1^s d_i, \\ V = \prod_{s+1}^t d_i. \end{array} \right.$$

Then, $UV = d = \frac{1}{4} + e$, where $e > 0$, and

$$\frac{\varphi(p-1)}{p-1} + \frac{\varphi(p+1)}{p+1} = \frac{1}{2} (U + V).$$

Therefore we must prove that $U + V > 1$.

Since $UV \neq \frac{1}{4}$ at least one of U and V will be $\neq \frac{1}{2}$:

Let $U = \frac{1}{2} + c$, where $c \neq 0$. Then

$$\begin{aligned} U + V &= U + \frac{d}{U} = \frac{U^2 + d}{U} = \frac{1}{U} \left(\frac{1}{4} + c + c^2 + \frac{1}{4} + e \right) = \\ &= \frac{1}{U} (U + c^2 + e) = 1 + \frac{c^2 + e}{U} > 1. \end{aligned}$$

Hence, $d > \frac{1}{4}$, and we can write now

$$2 \left(\frac{\varphi(p-1)}{p-1} + \frac{\varphi(p+1)}{p+1} \right) > 2 \left(\frac{\varphi(p-1)}{p-1} + \frac{\varphi(p+1)}{p+1} \right) = U + V > 1$$

which means

$$\varphi(p-1) + \varphi(p+1) > \frac{1}{2} (p-1).$$

We now consider a prime number p , such that $N = p^2 - 1$ has at most 20 different odd prime factors $q_1, q_2, \dots, q_s$, $s \leq 20$. Then

$$d = \prod_1^s \frac{q_i - 1}{q_i} > \frac{2}{3} \cdot \frac{4}{5} \dots \frac{72}{73} > 0.2521 > \frac{1}{4}.$$

Therefore

$$d > \frac{1}{4} \text{ and } \frac{\varphi(p-1)}{p-1} + \frac{\varphi(p+1)}{p+1} > \frac{1}{2}.$$

Finally observe that for any prime p which is less than $(3.5) \cdot 10^{15}$, N cannot have more than 20 different odd prime factors. Indeed, one has $p < (3.5) \cdot 10^{15}$ implies

$$p < \sqrt{8 \cdot 3 \cdot 5 \cdot 7 \dots 79}.$$

So that,

$$\frac{p^2 - 1}{8} < 3 \cdot 5 \cdot 7 \dots 79$$

where 79 is the 21th prime number.

BIBLIOGRAPHY

- [1] R. FRUCHT, *Generadores de $GF(p^2)$* , Rev. Soc. Mat. de Chile, **1**, no. 1 (1974), pp. 4, 18.
- [2] R. GIUDICI - H. LEON, *Generadores especiales y asociados de $GF(p^2)$* , Communication presented to the IV Escuela de Algebra, Sao Paulo, Brasil (1976), pp. 1-20.
- [3] E. JACOBSTHAL, *Über die darstellung der primzahlen der form $4n + 1$ als summe zweier quadrate*, J. Reine Angew. Math., **132** (1907), pp. 238, 245.

Manoscritto pervenuto in redazione il 5 aprile 1979.