UNIVERSITÄT KAISERSLAUTERN

# ON COMPLETELY FREE ELEMENTS IN FINITE FIELDS

Dirk Hachenberg

Preprint Nr. 232

FACHBEREICH MATHEMATIK

# ON COMPLETELY FREE ELEMENTS IN FINITE FIELDS

Dirk Hachenberger

Preprint Nr. 232

UNIVERSITÄT KAISERSLAUTERN
Fachbereich Mathematik
Erwin–Schrödinger–Straße
6750 Kaiserslautern

November 1992

# On Completely Free Elements in Finite Fields

Dirk Hachenberger
Fachbereich Mathematik der Universität Kaiserslautern
Erwin Schrödinger Straße
6750 Kaiserslautern
Federal Republik of Germany

**Abstract.** We show that the different module structures of $GF(q^m)$ arising from the intermediate fields of $GF(q^m)$ and $GF(q)$ can be studied simultaneously with the help of some basic properties of cyclotomic polynomials.

We use this ideas to give a detailed and constructive proof of the most difficult part of a Theorem of D. Blessenohl and K. Johnsen (1986), i.e., the existence of elements v in $GF(q^m)$ over $GF(q)$ which generate normal bases over any intermediate field of $GF(q^m)$ and $GF(q)$, provided that m is a prime power. Such elements are called completely free in $GF(q^m)$ over $GF(q)$.

We develop a recursive formula for the number of completely free elements in $GF(q^m)$ over $GF(q)$ in the case where m is a prime power.

Some of the results can be generalized to finite cyclic Galois extensions over arbitrary fields.

**AMS subject classification.** 11T30, 12E20.

## 1. Introduction. Cyclic Module Structures in Finite Fields.

In order to fix the notation, we summarize some basic results about finite fields, first. More details and proofs may be found in LIDL/NIEDERREITER (1983). For the general algebraic background we refer to JACOBSON (1985).

Let $q>1$ be a prime power and $m>1$ an integer; let $GF(q^m)$ be the Galois field of order $q^m$ and $\sigma : GF(q^m) \longrightarrow GF(q^m)$, $v \longrightarrow v^q$ the Frobenius automorphism of $GF(q^m)$ over $GF(q)$. The Galois group of $GF(q^m)$ over $GF(q)$ is cyclic of order m and is generated by $\sigma$.

The intermediate subfields of $GF(q^m)$ over $GF(q)$ are in one-to-one correspondence to the positive divisors of m. Let d be a positive divisor of m. The Galois group of $GF(q^m)$ over $GF(q^d)$ is generated by $\sigma^d$ and has order m/d. Since $\sigma^d$ in particular is a $GF(q^d)$-linear automorphism on $GF(q^m)$ (considered as an m/d-dimensional vector space over $GF(q^d)$), we know from Linear Algebra that $GF(q^m)$ becomes a $GF(q^d)[x]$-module with scalar multiplication

$$(1.1) \qquad (f,v)_d := f(\sigma^d)(v) = \sum_{i:=0}^{\deg(f)} f_i \, \sigma^{di}(v) = \sum_{i:=0}^{\deg(f)} f_i v^{q^{di}} ,$$

where f is a polynomial in $GF(q^d)[x]$, the polynomial ring in the indeterminate x over the field $GF(q^d)$, and v an element of $GF(q^m)$. (As usual, deg(f) denotes the degree of f.)

The minimal polynomial $\mu(\sigma^d)$ of $\sigma^d$ over $GF(q^d)$ is equal to $x^{m/d} - 1$. Furthermore, $GF(q^m)$ is a cyclic $GF(q^d)[x]$-module (as such denoted by $GF(q^m, q^d, \sigma^d)$). Any generator b of $GF(q^m, q^d, \sigma^d)$ is called a **free element in $GF(q^m)$ over $GF(q^d)$**. If b is free in $GF(q^m)$ over $GF(q^d)$, the set $\{b, \sigma^d(b), \sigma^{2d}(b), \ldots, \sigma^{m-d}(b)\}$ builds a $GF(q^d)$-basis of $GF(q^m)$, i.e. a **normal basis in $GF(q^m)$ over $GF(q^d)$**. For any v in $GF(q^m)$ let $\mu(\sigma^d, v)$ be the minimal polynomial of v over $GF(q^d)$, i.e. the monic polynomial g of least degree in $GF(q^d)[x]$, such that $(g,v)_d = 0$. It is a divisor of $x^{m/d} - 1$ and called the $q^d$-order of v.

The $GF(q^d)[x]$-submodules of $GF(q^m,q^d,\sigma^d)$ are in one-to-one correspondence to the monic divisors of $x^{m/d}-1$ in $GF(q^d)[x]$, i.e. let f be a monic divisor of $x^{m/d}-1$ in $GF(q^d)[x]$, then $U(\sigma^d,f) := \{ v \in GF(q^m,q^d,\sigma^d) \mid (f,v)_d = 0 \}$ is the $GF(q^d)$-submodule of $GF(q^m,q^d,\sigma^d)$ corresponding to f. $U(\sigma^d,f)$ is cyclic with minimal polynomial f and has order $q^{d\,\deg(f)}$. Furthermore, the elements of $U(\sigma^d,f)$ are exactly the roots of $\sum_{i:=0}^{\deg(f)} f_i x^{q^{di}}$, the associated $q^d$-polynomial of f. Finally, let $\Phi(q^d,f)$ denote the number of generators of $U(\sigma^d,f)$, i.e. the number of elements v in $GF(q^m)$ satisfying $\mu(\sigma^d,v) = f$. It is well known (see e.g. LIDL/NIEDERREITER (1983, Lemma 3.69)) that

$$\Phi(q^d,f) = \prod_{i:=1}^{a} \left( q^{d\,k_i \deg(f_i)} - q^{d\,(k_i-1)\deg(f_i)} \right), \tag{1.2}$$

where $\prod_{i:=1}^{a} f_i^{k_i}$ is the complete factorization of f over $GF(q^d)$.

The aim of this paper is to investigate simultaneously the different module structures of $GF(q^m)$. In the next section we prove some fundamental properties concerning the relation of the modules $GF(q^m,q,\sigma)$ and $GF(q^m,q^d,\sigma^d)$, where d is a positive divisor of m.

It is an interesting problem, not only because of the various applications of normal bases in practice, to consider the existence and the nature of elements v in $GF(q^m)$ which are free over any intermediate field between $GF(q)$ and $GF(q^m)$. We call such elements **completely free in GF($q^m$) over GF(q)**. The existence problem for arbitrary finite Galois extensions over any field was solved in BLESSENOHL/JOHNSEN (1986). In particular, concerning finite fields we have

**1.1 Theorem (D. Blessenohl, K. Johnsen, 1986).** Let $q>1$ be a prime power and $m>1$ an integer. There exist elements in $GF(q^m)$ which are completely free over $GF(q)$.

Using essentially our observations from section 2, in section 3 we will give a proof of the most difficult part of this theorem, namely the existence of a completely free element in $GF(q^m)$ over $GF(q)$ in the case where m is a prime power. As we will see, in this special case it is enough to be able to handle simultaneously the modules $GF(q^{r^n},q,\sigma)$ and $GF(q^{r^n},q^r,\sigma^r)$, with r being a prime number and $n \geq 2$ an integer.

Our approach to this problem is based on the results of section 2, on some properties of cyclotomic polynomials, the structure of the unit groups of the rings $\mathbb{Z}/n\mathbb{Z}$ of residues modulo n ( $\mathbb{Z}$ denotes the ring of integers ) and, of course, on the Chinese Remainder Theorem while D. Blessenohl and K. Johnsen in their (1986)-paper beside the structure of the unit groups of $\mathbb{Z}/n\mathbb{Z}$ mainly use representation theory of finite abelian groups. Although their proof could slightly be condensed in BLESSENOHL (1990), our approach still seems to be more natural. Furthermore, our proof is constructive; in particular, we are able to give a recursive formula for the number of completely free elements in $GF(q^m)$ over $GF(q)$, provided that m is a prime power.

## 2. **Basics.**

In this section we begin to study $GF(q^m)$ simultaneously as $GF(q)[x]$- and as $GF(q^d)[x]$-module for some positive divisor d of m.

**2.1 Theorem.** Let f be a monic divisor of $x^{m/d}-1$ in $GF(q)[x]$. Then $f(x^d)$ is a monic divisor of $x^m-1$ in $GF(q)[x]$. Furthermore, the modules $U(\sigma,f(x^d))$ and $U(\sigma^d,f)$ are equal as sets.

Conversely, if g is a monic divisor of $x^{m/d}-1$ in $GF(q^d)[x]$ and f is a monic divisor of $x^m-1$ in $GF(q)[x]$, such that the modules $U(\sigma,f)$ and $U(\sigma^d,g)$ coincide as sets, then g has actually coefficients in $GF(q)$ and $f=g(x^d)$ holds.

**Proof.** The first assertion is trivial. The equality of $U(\sigma,f(x^d))$ and $U(\sigma^d,f)$ as sets follows immediately from the fact that $(f,v)_d = (f(x^d),v)_1$ for any v in $GF(q^m)$ (observe that f has coefficients in $GF(q)$ by assumption).

Assume conversely that $U(\sigma,f)$ and $U(\sigma^d,g)$ are equal as sets for two polynomials g and f satisfying the assumptions. Let G and F be the associated $q^d$-polynomial of g and the associated q-polynomial of f, respectively. Now G and F are monic polynomials of degree $|U(\sigma,f)| = |U(\sigma^d,g)| = q^{\deg(f)} = q^{d\deg(g)}$. Since they have $q^{\deg(f)}$ common roots, we immediately obtain that $F = G$. Now it is obvious that g has coefficients in $GF(q)$ and that furthermore $f = g(x^d)$. □

As mentioned in the introduction, the modules $U(\sigma,f(x^d))$ and $U(\sigma^d,f)$ both are cyclic. In particular we are interested in completely free normal bases, so that generally we have to consider elements v which simultaneously generate both modules. We therefore next give an easy criterion to decide if $\mu(\sigma^d,v)=f$ provided that $\mu(\sigma,v)=f(x^d)$.

**2.2 Lemma.** Let f be a monic divisor of $x^{m/d}-1$ with coefficients in $GF(q)$. Let $v\in GF(q^m)$ with $\mu(\sigma,v)=f(x^d)$. Then $\mu(\sigma^d,v)$ is a monic divisor of f. Furthermore, $\mu(\sigma^d,v)=f$ if and only if $\mu(\sigma^d,v)$ has coefficients in $GF(q)$.

**Proof.** Let f be a monic divisor of $x^{m/d}-1$ in $GF(q)[x]$ and $v\in GF(q^m)$ with $\mu(\sigma,v)=f(x^d)$. As a consequence of Theorem 2.1, v is an element of $U(\sigma^d,f)$ and therefore $\mu(\sigma^d,v)$ is a divisor of f.

Of course, one if-part is trivial. Let therefore $\mu(\sigma^d,v)$ be a polynomial over $GF(q)$. Then $(\mu(\sigma^d,v)(x^d),v)_1 = (\mu(\sigma^d,v),v)_d = 0$ and therefore $f(x^d)=\mu(\sigma,v)$ is a divisor of $\mu(\sigma^d,v)(x^d)$. Comparing degrees, we obtain

$$d\deg(f) = \deg(f(x^d)) \le \deg(\mu(\sigma,v)(x^d)) = d\deg(\mu(\sigma,v)) \le d\deg(f).$$

Therefore equality holds everywhere and we get that $\deg(f) = \deg(\mu(\sigma^d, v))$. Since both polynomials are monic and $\mu(\sigma^d, v)$ is a divisor of f, we obtain $f = \mu(\sigma^d, v)$. □

The following applications of Lemma 2.2 are very useful.

**2.3 Corollary.** Let $v \in GF(q^m)$ be free over GF(q). Let d be a positive divisor of m. Then v is free over $GF(q^d)$ if and only if $\mu(\sigma^d, v)$ has coefficients in GF(q). □

Furthermore, we have

**2.4 Corollary.** Let f be a monic divisor of $x^{m/d} - 1$ in $GF(q^d)[x]$. Assume that any irreducible divisor of f in $GF(q^d)[x]$ actually has coefficients in GF(q). Then any element v with $\mu(\sigma, v) = f(x^d)$ has $q^d$-order f.

In particular, if all irreducible factors of $x^{m/d} - 1$ in $GF(q^d)[x]$ actually have coefficients in GF(q), then any free element in $GF(q^m)$ over GF(q) remains free over $GF(q^d)$. □

## 3. The Number and Existence of Completely Free Elements in Field Extensions of Prime Power Degree over GF(q).

Again, let $q>1$ be a prime power; let furthermore r be a prime number and $n\geq 1$ an integer. The main problem in the proof of the Theorem of Blessenohl and Johnsen (see 1.1) is to show the existence of completely free elements in $GF(q^{r^n})$ over GF(q). This will be done constructively in this section. The general existence result then follows from Theorem 3.1, which reduces the general existence problem to the case where the degree of the extension is a prime power. For a proof of Theorem 3.1, we refer to BLESSENOHL/JOHNSEN (1986) and further literature stated there.

**3.1 Theorem.** Let m be a positive integer and let $\prod_{i:=1}^{k} p_i^{a_i}$ be the prime factorization of m. Let $q>1$ be any prime power. If $v_i$ is completely free in $GF(q^{p_i^{a_i}})$ over GF(q) for any $i := 1,\dots,k$, then $v := \prod_{i:=1}^{k} v_i$ is completely free in $GF(q^m)$ over GF(q). ¤

We start to introduce some notation. Let

$$\underline{\Gamma(q,r^n)} \tag{3.1}$$

be the number of completely free elements in $GF(q^{r^n})$ over GF(q), i.e. the number of elements v in $GF(q^{r^n})$ satisfying

$$\mu(\sigma^{r^i},v) = x^{r^{n-i}}-1 \qquad \text{for } 0\leq i\leq n-1. \tag{3.2}$$

(Remember that σ is the Frobenius automorphism of $GF(q^{r^n})$ over GF(q).)

Let $Q(r^i)$ denote the $r^i$-th cyclotomic polynomial and let

$$\underline{\Omega(q,r^n)} \tag{3.3}$$

be the number of elements v in $GF(q^{r^n})$ satisfying

$$\mu(\sigma^{r^i},v) = Q(r^{n-i}) \qquad \text{for } 0\leq i\leq n-1. \tag{3.4}$$

Furthermore, recall from section 1 that the number of free elements in $GF(q^{r^n})$ over GF(q) is denoted by

$$\underline{\Phi(q,x^{r^n}-1).} \tag{3.5}$$

We have to consider two cases, the first of which is easy to handle.

**3.2 Theorem.** Assume that r is equal to the characteristic of GF(q). Then any free element in $GF(q^{r^n})$ over GF(q) is completely free.

In particular $\Gamma(q,p^n) = \Phi(q,x^{r^n}-1) = q^{r^n} - q^{r^{n-1}}$.

**Proof.** Since r is the characteristic of GF(q), we have that $x^{r^i}-1 = (x-1)^{r^i}$ for all non-negative integers i. Hence this polynomial splits over GF(q) and therefore $\mu(\sigma^{r^i},v)$ has coefficients in GF(q) for any $0 \le i \le n-1$ and any v in $GF(q^{r^n})$. Now the assertion follows from Corollary 2.4 and (1.2). □

From now on we assume that r is different from the characteristic of GF(q). In this case the polynomial $x^{r^n}-1$ has no multiple roots over GF(q). Using repeatedly the Chinese Remainder Theorem, we next give a fundamental characterization of completely free elements in $GF(q^{r^n})$ over GF(q).

**3.3 Theorem.** Let $v \in GF(q^{r^n})$. Then there exist unique elements $v_1$ and $v_2$ in $GF(q^{r^n})$ such that $v = v_1 + v_2$, $\mu(\sigma,v_1)$ divides $x^{r^{n-1}}-1$ and $\mu(\sigma,v_2)$ divides $Q(r^n)$. Furthermore, v is completely free in $GF(q^{r^n})$ over GF(q) if and only if $v_1$ is completely free in $GF(q^{r^{n-1}})$ over GF(q) and $v_2$ satisfies (3.4).

**Proof.** Let $v \in GF(q^{r^n})$. Then $\mu(\sigma,v)$ divides $x^{r^n}-1$ and $\mu(\sigma,v) = x^{r^n}-1$ if and only if v is free over GF(q). Since $x^{r^n}-1 = (x^{r^{n-1}}-1)\,Q(r^n)$ and $x^{r^{n-1}}-1$ and $Q(r^n)$ are relatively prime, the Chinese Remainder Theorem guarantees the existence of $v_1$ and $v_2$ satisfying the assertions in the first statement.

Now let v be completely free in $GF(q^{r^n})$ over GF(q). Since v is free over GF(q), we have that $\mu(\sigma,v_1) = x^{r^{n-1}}-1$ and $\mu(\sigma,v_2) = Q(r^n)$ by the Chinese Remainder Theorem. Let $0 \le i \le n-1$. As $x^{r^{n-1}}-1 = (x^{r^i})^{r^{n-1-i}}-1$ and $Q(r^n) = Q(r^{n-i})(x^{r^i})$ (for basic properties of cyclotomic polynomials see e.g. LIDL/NIEDERREITER (1983, Exercise 2.57)), it follows from Theorem 2.1 that $\mu(\sigma^{r^i},v_1)$ divides $x^{r^{n-1-i}}-1$ while $\mu(\sigma^{r^i},v_2)$ divides $Q(r^{n-i})$. As $\mu(\sigma^{r^i},v) = x^{r^{n-i}}-1$ by assumption, the Chinese Remainder Theorem implies $\mu(\sigma^{r^i},v_1) = x^{r^{n-1-i}}-1$ and $\mu(\sigma^{r^i},v_2) = Q(r^{n-i})$. Since this holds for any i, we see that $v_1$ is completely free in $GF(q^{r^{n-1}})$ over GF(q) while $v_2$ satisfies (3.4).

The converse likewise follows immediately using the Chinese Remainder Theorem. Let $v_1$ be completely free in $GF(q^{r^{n-1}})$ over GF(q) and assume that $v_2$ satisfies (3.4). Then $\mu(\sigma^{r^i},v_1) = x^{r^{n-1-i}}-1$ and $\mu(\sigma^{r^i},v_2) = Q(r^{n-i})$ and therefore $\mu(\sigma^{r^i},v) = x^{r^{n-i}}-1$ for all $0 \le i \le n-1$, wherefore v satisfies (3.2) and is completely free in $GF(q^{r^n})$ over GF(q). □

Recursively, we obtain

**3.4 Corollary.** Let v be a completely free element in $GF(q^{r^n})$ over $GF(q)$. Then v can uniquely be written as $\sum_{i:=0}^{n} v_i$, where $\mu(\sigma, v_0) = x-1$, i.e. $v_0 \in GF(q)-\{0\}$, and $\mu(\sigma^{r^i}, v_j) = Q(r^{j-i})$ for all $0 \le i \le j-1$ and all $1 \le j \le n$.

Furthermore, for any $1 \le j \le n$, the element $w_j = \sum_{i:=0}^{j} v_i$ is completely free in $GF(q^{r^j})$ over $GF(q)$.

In particular, $\Gamma(q, r^n) = \Phi(q, x-1) \prod_{j:=1}^{n} \Omega(q, r^j)$. □

Since $x^r - 1 = (x-1)Q(r)$ and $Q(r)$ over $GF(q)$ splits into the product of $(r-1)/\text{ord}(r;q)$ distinct irreducible polynomials each of degree $\text{ord}(r;q)$, the multiplicative order of q modulo r (i.e. the multiplicative order of $q + r\mathbb{Z}$ in the ring $\mathbb{Z}/r\mathbb{Z}$ of residues modulo r), we obtain from (1.2) that

$$\begin{aligned}\Phi(q, x-1)\,\Omega(q, r) &= \Phi(q, x-1)\,\Phi(q, Q(r)) \\ &= (q-1)\,(q^{\text{ord}(r;q)} - 1)^{(r-1)/\text{ord}(r;q)},\end{aligned}$$

(see e.g. LIDL/NIEDERREITER (1983, Theorem 2.47)). It therefore remains to determine the number $\Omega(q, r^n)$, where $n \ge 2$. This will be done in the sequel.

In order to handle the problem, we have to point out the difficulties in turning from $GF(q)$ to $GF(q^r)$ as ground fields, i.e. in studying the modules $GF(q^{r^n}, q, \sigma)$ and $GF(q^{r^n}, q^r, \sigma^r)$ simultaneously. To this purpose, remembering the content of Theorem 2.1, let $g_1 g_2 \ldots g_a$ be the complete factorization of $Q(r^{n-1})$ over $GF(q)$. Since $n \ge 2$, we have that $Q(r^n) = Q(r^{n-1})(x^r) = g_1(x^r) g_2(x^r) \ldots g_a(x^r)$. By the Chinese Remainder Theorem, any element w in $GF(q^{r^n})$ over $GF(q)$ satisfying $\mu(\sigma, w) = Q(r^n)$ and $\mu(\sigma^r, w) = Q(r^{n-1})$ can uniquely be written as $\sum_{i:=1}^{a} w_i$ where $\mu(\sigma, w_i) = g_i(x^r)$ and $\mu(\sigma^r, w_i) = g_i$ for all $1 \le i \le a$. Therefore, for any i we have to find elements of q-order $g_i(x^r)$ and $q^r$-order $g_i$.

Let furthermore $h_1 h_2 \ldots h_b$ be the complete factorization of $Q(r^{n-1})$ over $GF(q^r)$ and $f_1 f_2 \ldots f_c$ the complete factorization of $Q(r^n)$ over $GF(q)$. We know that

$$\begin{aligned}
&a = \varphi(r^{n-1})/\text{ord}(r^{n-1};q) && \text{and} && \deg(g_i) = \text{ord}(r^{n-1};q) \text{ for } 1 \le i \le a, \\
&b = \varphi(r^{n-1})/\text{ord}(r^{n-1};q^r) && \text{and} && \deg(h_i) = \text{ord}(r^{n-1};q^r) \text{ for } 1 \le i \le b\,, \\
&c = \varphi(r^n)/\text{ord}(r;q) && \text{and} && \deg(f_i) = \text{ord}(r^n;q) \text{ for } 1 \le i \le c.
\end{aligned}$$

($\varphi$ denotes the Euler function, i.e. $\varphi(n)$ is the number of units in the ring $\mathbb{Z}/n\mathbb{Z}$.) We will see that the parameters of each decomposition depend only on $\mathrm{ord}(r^n;q)$. Let $U(\mathbb{Z}/r^n\mathbb{Z})$ be the group of units of the ring $\mathbb{Z}/r^n\mathbb{Z}$. This group has order $\varphi(r^n) = r^{n-1}(r-1)$. Therefore $\mathrm{ord}(r^n;q)$ has the form $r^k u$, where $0 \leq k \leq n-1$ and u is a divisor of $r-1$.

Now let g be any irreducible factor of $Q(r^{n-1})$ over $GF(q)$. We want to find the number of elements v in $GF(q^{r^n})$ satisfying $\mu(\sigma,v) = g(x^r)$ and $\mu(\sigma^r,v) = g$. It will turn out that this number is independent of the choice of g.

There are two cases which are easy to handle, they have obvious solution.

**Case I.** Assume that $g(x^r)$ is irreducible over $GF(q)$.

Let $v \in GF(q^{r^n})$. If $\mu(\sigma^r,v) = g$, then $v \neq 0$ and therefore $\mu(\sigma,v) \neq 1$. Theorem 2.1 implies that $\mu(\sigma,v)$ divides $g(x^r)$ and therefore, by the irreducibility of $g(x^r)$, we have that $\mu(\sigma,v) = g(x^r)$. Hence, in this case, any element of $q^r$-order g has q-order $g(x^r)$.

Now $g(x^r)$ is irreducible over $GF(q)$ if and only if $a=c$, i.e. if and only if $\varphi(r^n)/\mathrm{ord}(r^n;q) = r\varphi(r^{n-1})/\mathrm{ord}(r^n;q) = \varphi(r^{n-1})/\mathrm{ord}(r^{n-1};q)$, i.e. if and only if

(3.6) $$\mathrm{ord}(r^{n-1};q) = \mathrm{ord}(r^n;q)/r$$

holds. In particular, r divides the order of q modulo $r^n$.

This criterium is independent of the choice of g and satisfied if and only if

(3.6') the subgroup of $U(\mathbb{Z}/r^n\mathbb{Z})$ generated by $q+r^n\mathbb{Z}$ contains the kernel of the natural epimorphism

$$\eta : U(\mathbb{Z}/r^n\mathbb{Z}) \longrightarrow U(\mathbb{Z}/r^{n-1}\mathbb{Z}),\ u+r^n\mathbb{Z} \longrightarrow u+r^{n-1}\mathbb{Z}.$$

Assuming (3.6) and applying the Chinese Remainder Theorem as mentioned above and in the same way, it has been used in the proof of Theorem 3.3, we obtain that $\mu(\sigma^r,w) = Q(r^{n-1})$ implies that $\mu(\sigma,w) = Q(r^n)$ and therefore

$$\Omega(q,r^n) = \Omega(q^r,r^{n-1})$$

holds. We may therefore reduce the problem to a field extension of smaller prime power degree. □

**Case II.** Assume that g remains irreducible over $GF(q^r)$.

Let $v \in GF(q^{r^n})$. If $\mu(\sigma,v)=g(x^r)$, then v is different from 0 and therefore, since g is irreducible over $GF(q^r)$, $\mu(\sigma^r,v)$ is equal to g. Hence, in this case, we obtain that any element of q-order $g(x^r)$ has $q^r$-order g.

Now g is irreducible over $GF(q^r)$ if and only if $a=b$, i.e. if and only if $\varphi(r^{n-1})/\mathrm{ord}(r^{n-1};q) = \varphi(r^{n-1})/\mathrm{ord}(r^{n-1};q^r)$, i.e. if and only if

$$\mathrm{ord}(r^{n-1};q) = \mathrm{ord}(r^{n-1};q^r) \tag{3.7}$$

holds.

Again, this criterium is independent of the choice of g. It is satisfied if and only if

(3.7') r does not divide the order of $q+r^{n-1}\mathbb{Z}$ in $U(\mathbb{Z}/r^{n-1}\mathbb{Z})$.

The consequence of this case is the content of the following theorem.

**3.5 Theorem.** Let q be a prime power, r a prime number which does not divide q and $n \geq 2$ an integer. Assume that r does not divide $\mathrm{ord}(r^{n-1};q)$, the order of q modulo $r^{n-1}$. Then any free element in $GF(q^{r^n})$ over $GF(q)$ is completely free over $GF(q)$ and therefore

$$\Gamma(q,r^n) = \Phi(q,x^{r^n}-1) \text{ and}$$

$$\Omega(q,r^n) = \Phi(q;Q(r^n)) = \left(q^{\mathrm{ord}(r^n;q)}-1\right)^{r^{n-1}(r-1)/\mathrm{ord}(r^n;q)}$$

hold.

In particular, any free element in $GF(q^{r^2})$ over $GF(q)$ is completely free.

**Proof.** Assume that r does not divide $\mathrm{ord}(r^{n-1};q)$, then r does not divide $\mathrm{ord}(r^i;q)$ for any $1 \leq i \leq n-1$. Furthermore, for any integer $j \geq 0$ the order of $q^{r^j}$ modulo $r^i$ is equal to $\mathrm{ord}(r^i;q)$ for all $1 \leq i \leq n-1$ and therefore likewise not divisible by r. As a consequence of this, for any $1 \leq i \leq n-1$, the factorization of $x^{r^{n-i}}-1$ over $GF(q^{r^i})$ is the same as over $GF(q)$. We may therefore apply Corollary 2.4 and obtain that any free element in $GF(q^{r^n})$ over $GF(q)$ is completely free over $GF(q)$. This proves the assertion. Now the equations for $\Gamma(q,r^n)$ and $\Omega(q,r^n)$ follow from the definitions (3.1) to (3.5) and (1.2).

If $n=2$, the assumptions are always satisfied, since $\mathrm{ord}(r;q)$ divides $\varphi(r) = r-1$ and therefore is not divisible by r. We obtain that any free element in $GF(q^{r^2})$ over $GF(q)$ is completely free. □

It remains to consider the **critical case**, i.e. the case where neither $g(x^r)$ nor g is irreducible in $GF(q)[x]$ and $GF(q^r)[x]$, respectively. Because of (3.6') we start with determining those situations, where $\langle q+r^n\mathbb{Z}\rangle$, the subgroup of $U(\mathbb{Z}/r^n\mathbb{Z})$ generated by $q+r^n\mathbb{Z}$, contains the kernel of $\eta$. We use the following theorem, a proof of which can be found in LÜNEBURG (1978, 7).

**3.6 Theorem.** Let r be a prime number and $n \geq 1$ an integer. Then $U(\mathbb{Z}/r^n\mathbb{Z})$ is cyclic if and only if r is odd or $r^n \in \{2,4\}$, while $U(\mathbb{Z}/2^n\mathbb{Z})$ is a direct product of the cyclic subgroups $U_1 := \langle 5+2^n\mathbb{Z}\rangle$ and $U_2 := \langle -1+2^n\mathbb{Z}\rangle$ of order $2^{n-2}$ and 2, respectively, provided that $n \geq 3$. ⌗

Remember that $r^k$ is the maximal r-power dividing $\mathrm{ord}(r^n;q)$. The kernel of $\eta$ is equal to $\langle 1+r^{n-1}+r^n\mathbb{Z}\rangle$ and has order r. Therefore, a necessary condition for (3.6') is that r divides $\mathrm{ord}(r^n;q)$, i.e. we assume that the parameter k is at least 1.

It is obvious that (3.6') holds, provided that $U(\mathbb{Z}/r^n\mathbb{Z})$ is cyclic, since then there is only one subgroup in $U(\mathbb{Z}/r^n\mathbb{Z})$ of order r, namely the kernel of $\eta$.

By Theorem 3.6, let therefore $n\geq3$ and $r=2$. In this case (see LÜNEBURG (1978, 7)), we have that the kernel of $\eta$ is equal to $\langle 5^{2^{n-3}}+2^n\mathbb{Z}\rangle$ and has order 2. Consequentely, it is the unique subgroup of order 2 of $U(\mathbb{Z}/2^n\mathbb{Z})^2 = \{x^2 + 2^n\mathbb{Z} \mid x \in \mathbb{Z},\ x \text{ odd}\}$. Therefore, if $\mathrm{ord}(2^n;q)$ is divisible by 4, the subgroup $\langle q+2^n\mathbb{Z}\rangle$ likewise contains the kernel of $\eta$. Hence (3.6') holds, provided that $k\geq 2$. Trivially, if $\mathrm{ord}(2^n;q) = 2$ and $q \equiv 5^{2^{n-3}} \bmod 2^n$, then $\langle q+2^n\mathbb{Z}\rangle$ contains the kernel of $\eta$.

Altogether we conclude that (3.6) does not hold if and only if $k=0$ or ($r=2$, $k=1$, $n\geq3$ and $q \not\equiv 5^{2^{n-3}} \bmod 2^n$). The latter case is called the **exceptional case** in BLESSENOHL/JOHNSEN (1986).

If $k=0$ then $\mathrm{ord}(r^n;q) = \mathrm{ord}(r^{n-1};q) = \mathrm{ord}(r^{n-1};q^r)$ and we have Case II which is covered by Theorem 3.5.

Summarizing our results, we see that

(3.8) the only critical case is the exceptional case. □

In the following theorem the exceptional case is handled.

**3.7 Theorem.** Assume the exceptional case. Let $v \in GF(q^{2^n})$. Then $v$ satisfies (3.4) if and only if $\mu(\sigma,v)=Q(2^n)$ and $\mu(\sigma^2,v)=Q(2^{n-1})$. Furthermore,

$$\Omega(q,2^n) = (q^4 - 4q^2 + 3)^{2^{n-3}} > 0.$$

**Proof.** Assume that $q$ is odd and $ord(2^n;q) = 2$, where $n \geq 3$. Furthermore, let $q \not\equiv 5^{2^{n-3}} \bmod 2^n$. Then, over $GF(q)$, the polynomial $Q(2^{n-1})$ splits into the product of $2^{n-3}$ irreducible factors each of degree 2. Let $g$ be any irreducible divisor of $Q(2^{n-1})$ over $GF(q)$. Then $g(x^2)$ divides $Q(r^n)$ and, over $GF(q)$, is the product of two irreducible polynomials each of degree 2, while $g$ splits over $GF(q^2)$ into two linear factors, say $h_1$ and $h_2$.

Since $GF(q^2)$ is the splitting field of $Q(2^{n-1})$, we deduce that $x^{2^{n-1}}-1$ splits into linear factors over $GF(q^2)$. Therefore, an application of Corollary 2.4 shows that any free element in $GF(q^{2^n})$ over $GF(q^2)$ is completely free. This implies that $v$ satisfies (3.4) if and only if $\mu(\sigma,v)=Q(2^n)$ and $\mu(\sigma^2,v)=Q(2^{n-1})$, i.e. the first assertion.

We want to determine the number of elements $v$ satisfying $\mu(\sigma,v)=g(x^2)$ and $\mu(\sigma^2,v)=g$. To this end let $h := x-\zeta$ be a linear factor of $g$ over $GF(q^2)$ and $f := x^2 - \alpha x - \beta$ an irreducible factor of $g(x^2)$ over $GF(q)$. If $\mu(\sigma,v)=f$ and $\mu(\sigma^2,v)=h$, we obtain

$$\sigma^2(v) - \zeta v = (x-\zeta,v)_2 = 0 = (x^2 - \alpha x - \beta, v)_1 = \sigma^2(v) - \alpha\sigma(v) - \beta v$$

and therefore $\zeta v = \alpha\sigma(v)+\beta v$. Since $\zeta \in GF(q^2)-GF(q)$ and $v \neq 0$, we have that $\alpha$ is not equal to 0. Therefore, $\sigma(v) = \nu v$, where $\nu := (\zeta-\beta)/\alpha \in GF(q^2)-GF(q)$. Now

$$(x-\zeta,\sigma(v))_2 = \sigma^2(\sigma(v)) - \zeta\sigma(v) = \nu(\sigma^2(v)-\zeta v) = \nu(x-\zeta,v)_2 = 0$$

and since $\nu v \neq 0$, we see that $\deg(\mu(\sigma^2,\nu v)) > 0$ wherefore $\mu(\sigma^2,\nu v) = x-\zeta$. But on the other hand, we have that $\mu(\sigma^2,\nu v) = \mu(\sigma^2,\sigma(v)) = x - \sigma(\zeta)$, and so we obtain $\zeta = \sigma(\zeta)$. This is a contradiction to the fact that $\zeta$ does not lie in $GF(q)$.

We conclude that for any element $v$ with $\deg(\mu(\sigma^2,v)) = 1$ the minimal polynomial over $GF(q)$ is equal to $g(x^2)$. Now, using (1.2) we obtain

$$\begin{aligned} &\left| \{v \in GF(q^{2^n}) \mid \mu(\sigma,v)=g(x^2),\ \mu(\sigma^2,v)=g\} \right| \\ =\ & \Phi(q,g(x^2)) - \Phi(q^2,h_1) - \Phi(q^2,h_2) \\ =\ & (q^2-1)^2 - (q^2-1) - (q^2-1) \\ =\ & q^4 - 4q^2 + 3. \end{aligned}$$

This number is greater than 0 and independent of the choice of g, wherefore together with the Chinese Remainder Theorem (compare its application in Case I and the proof of Theorem 3.3) we obtain

$$\Omega(q,2^n) = \left|\{v \in GF(q^{2^n}) \mid \mu(\sigma,v) = Q(2^n),\ \mu(\sigma^2,v) = Q(2^{n-1})\}\right|$$
$$= (q^4 - 4q^2 + 3)^{2^{n-3}} > 0,$$

i.e. the assertion. □

**3.8 Example.** Let q be an odd prime power. We want to determine the number of completely free elements in $GF(q^8)$ over GF(q).

If $q \equiv 1 \bmod 8$ or $q \equiv 5 \bmod 8$, then $\Omega(q,8) = \Phi(q,Q(8))$ and $\Gamma(q,8) = \Phi(q,x^8-1)$ by Theorem 3.5, i.e. any free element in $GF(q^8)$ over GF(q) is completely free. Using (1.2), we have $\Gamma(q,8) = (q-1)^8$ in the first and $\Gamma(q,8) = (q-1)^4(q^2-1)^2$ in the second case.

If $q \equiv 3 \bmod 8$ or $q \equiv 7 \bmod 8$, we are in the exceptional case and therefore $\Omega(q,8) = q^4 - 4q^2 + 3$ by Theorem 3.7. Using Corollary 3.4, the formula (1.2) and Theorem 3.5, in both cases we get that $\Gamma(q,8) = (q-1)^2(q^2-1)(q^4-4q^2+3)$. Comparing this term with $\Phi(q,x^8-1)$, we obtain

$$\frac{\Gamma(q,8)}{\Phi(q,x^8-1)} = 1 - \frac{2}{q^2-1}.$$

E.g., if q = 3, then 3/4 of all free elements in $GF(3^8)$ over GF(3) are completely free over GF(3). □

Summarizing our results, we have a recursive formula for the number of elements in $GF(q^{r^n})$ satisfying (3.4) and, using Theorem 3.3 and Corollary 3.4, the existence of completely free elements in $GF(q^{r^n})$ over GF(q), as desired.

**3.9 Theorem.** Let q be a prime power, r a prime number different from the characteristic of GF(q) and $n \geq 1$ an integer. Let $\Phi$, $\Gamma$ and $\Omega$ as in (3.1) - (3.5).

If n = 1 or n = 2 then any free element in $GF(q^{r^n})$ over GF(q) is completely free.

Let $n \geq 3$. Any completely free element v in $GF(q^{r^n})$ over $GF(q)$ can uniquely be written as $v = v_1 + v_2$, where $v_1$ is completely free in $GF(q^{r^{n-1}})$ over $GF(q)$ and $v_2$ satisfies (3.4), i.e. $\mu(\sigma^{r^i}, v_2) = Q(r^{n-i})$ for all $0 \leq i \leq n-1$. The number $\Gamma(q,r^n)$ of completely free elements in $GF(q^{r^n})$ over $GF(q)$ is equal to

$$\Gamma(q,r^{n-1})\ \Omega(q,r^n).$$

Moreover, let $0 \leq k \leq n-1$ be defined by $\mathrm{ord}(r^n; q) = r^k u$, where u is a divisor of $r-1$.

(3.10) If $k=0$ or ( $k=1$ and (r is odd or ($r=2$ and $q \equiv 5^{2^{n-3}} \bmod 2^n$))), then

$$\Omega(q,r^n) = \Phi(q,\ Q(r^n)) = \left( q^{r^k u} - 1 \right)^{r^{n-1-k}(r-1)/u}.$$

Moreover, any free element in $GF(q^{r^n})$ over $GF(q)$ is completely free.

(3.11) If $k=1$ and $r=2$ and ($q \equiv -1 \bmod 2^n$ or $q \equiv -5^{2^{n-3}} \bmod 2^n$), then

$$\Omega(q,r^n) = (q^4 - 4q^2 + 3)^{2^{n-3}}.$$

(3.12) If $k \geq 2$ then

$$\Omega(q,r^n) = \Omega(q^r, r^{n-1}) \quad \text{and} \quad \mathrm{ord}(r^{n-1}; q^r) = r^{k-2}u.$$

In particular, there do exist completely free elements in $GF(q^{r^n})$ over $GF(q)$.

**Proof.** The only assertion which is left to prove is the equality $\mathrm{ord}(r^{n-1};q^r) = r^{k-2}u$ in (3.12). But this is obvious. Since $\langle q + r^n\mathbf{Z} \rangle$ contains the kernel of $\eta$ (see (3.6')), we obtain $\mathrm{ord}(r^{n-1};q) = r^{k-1}u$. This number is divisible by r and therefore, $\mathrm{ord}(r^{n-1};q^r) = \mathrm{ord}(r^{n-1};q)/r$. □

We conclude this section with a remark and a further example.

**3.10 Remark.** Assume that $n \geq 3$ and $r = 2$ and that $\mathrm{ord}(2^n;q)$ is divisible by 4, i.e. $k \geq 2$. By Theorem 3.6 we have that $U(\mathbf{Z}/2^n\mathbf{Z})^2 = \langle 5^2 + 2^n\mathbf{Z} \rangle$ contains $q^2 + 2^n\mathbf{Z}$. Turning over to the modulus $\mathbf{Z}/2^{n-1}\mathbf{Z}$, we see that $\langle q^2 + 2^{n-1}\mathbf{Z} \rangle$ is a subgroup of $\langle 5^2 + 2^{n-1}\mathbf{Z} \rangle = U(\mathbf{Z}/2^{n-1}\mathbf{Z})^2$ and therefore contains the kernel of $\gamma: U(\mathbf{Z}/2^{n-1}\mathbf{Z}) \longrightarrow U(\mathbf{Z}/2^{n-2}\mathbf{Z})$, $x + 2^{n-1}\mathbf{Z} \longrightarrow x + 2^{n-2}\mathbf{Z}$. Using induction we conclude that under our assumptions the exceptional case will never occur in recursion (3.12).

Therefore, in the general case, i.e. if q is any prime power, r a prime number which does not divide q, $n \geq 3$ an integer and $\mathrm{ord}(r^n;q) = r^k u$, where $k \geq 2$ and u divides $r-1$, we may use induction and (3.10) to give an explicit formula for $\Omega(q,r^n)$. Let $t := \max\{x \mid x \text{ an integer and } x \leq k/2\}$. Then, by (3.12), $\Omega(q,r^n) = \Omega(q^{r^t}, r^{n-t})$ and, after turning from GF(q) to GF($q^{r^t}$), Case II holds, wherefore we obtain altogether

(3.12') $$\Omega(q,r^n) = \Phi(q^{r^t}, Q(r^{n-t})), \qquad \text{if } k \geq 2 \text{ and } t \text{ as above.}$$

Using (1.2), after some simplifications, we see that this number is equal to

$$\left(q^{r^{k-t}u} - 1\right)^{\varphi(r^{n-t})/r^{k-2t}u}. \quad \square$$

**3.11 Example.** Let q be a prime power and r an odd prime number which does not divide q. Let $r^k u$, u a divisor of $r-1$, be the order of q modulo $r^3\mathbb{Z}$. Then $k \leq 2$. The number $\Gamma(q,r^3)$ of completely free elements in GF($q^{r^3}$) over GF(q) is equal to

$$\Phi(q, x^{r^3}-1), \qquad \text{if} \quad k < 2 \quad \text{and}$$

$$\Phi(q, x^{r^2}-1)\,\Phi(q^r, Q(r^2)), \qquad \text{if} \quad k = 2. \quad \square$$

**References.**

BLESSENOHL, D. and JOHNSEN, K. (1986), Eine Verschärfung des Satzes von der Normalbasis, *J. of Algebra 103*, 141 - 159.

BLESSENOHL, D. (1990), Supplement zu "Eine Verschärfung des Satzes von der Normalbasis", *J. of Algebra 132*, 154 - 159.

JACOBSON, N. (1985), Basic Algebra I. 2nd Ed., Freeman and Company, New York.

LIDL, R. and NIEDERREITER, H. (1983), Finite Fields. Addison - Wesley, Reading, Massachusetts.

LÜNEBURG, H. (1978), Vorlesungen über Zahlentheorie. Birkhäuser Verlag, Basel.