Designs, Codes and Cryptography, 4, 129-143 (1994)
© 1994 Kluwer Academic Publishers. Manufactured in The Netherlands.

On Completely Free Elements in Finite Fields

DIRK HACHENBERGER
*Lehrstuhl für Augewandte Mathematik II, Universität Augsburg, Universitätsstr. 8,
86135 Augsburg, Germany*

Communicated by D. Jungnickel
Received November 2, 1992; Revised June 30, 1993.

Abstract. Let $q > 1$ be a prime power, $m > 1$ an integer, $GF(q^m)$ and $GF(q)$ the Galois fields of order q^m and q, respectively. We show that the different module structures of $(GF(q^m), +)$ arising from the intermediate fields of the field extension $GF(q^m)$ over $GF(q)$ can be studied simultaneously with the help of some basic properties of cyclotomic polynomials. The results can be generalized to finite cyclic Galois extensions over arbitrary fields.

In 1986, D. Blessenohl and K. Johnsen proved that there exist elements in $GF(q^m)$ which generate normal bases in $GF(q^m)$ over *any* intermediate field $GF(q^d)$ of $GF(q^m)$ over $GF(q)$. Such elements are called completely free in $GF(q^m)$ over $GF(q)$. Using our ideas, we give a detailed and constructive proof of the most difficult part of that theorem, i.e., the existence of completely free elements in $GF(q^m)$ over $GF(q)$ provided that m is a prime power. The general existence problem of completely free elements is easily reduced to this special case.

Furthermore, 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.

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 and Niederreiter [6, Chap. 1, 2]. For the general algebraic background we refer to Jacobson [4].

Let $q > 1$ be a prime power and $m > 1$ an integer; let $GF(q^m)$ and $GF(q)$ be the Galois fields of order q^m and q, respectively. Let σ: $GF(q^m) \rightarrow GF(q^m)$, $v \rightarrow v^q$ be 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 σ.

The intermediate fields of $GF(q^m)$ over $GF(q)$ are exactly the fields $GF(q^d)$, where $d \geq 1$ is a divisor of m. The Galois group of $GF(q^m)$ over $GF(q^d)$ is cyclic of order $\frac{m}{d}$ and is generated by σ^d. Since σ^d in particular is a $GF(q^d)$-linear automorphism on $GF(q^m)$, considered as an $\frac{m}{d}$-dimensional vector space over $GF(q^d)$, we know from Linear Algebra that $(GF(q^m), +)$, the additive group of $GF(q^m)$, becomes a $GF(q^d)[x]$-module with scalar multiplication

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

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

The minimal polynomial $\mu(\sigma^d)$ of σ^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 of $GF(q^m, q^d, \sigma^d)$ is called a *free element in* $GF(q^m)$ over $GF(q^d)$. If w is free in $GF(q^m)$ over $GF(q^d)$, the set

$$\{w, \sigma^d(w), \sigma^{2d}(w), \ldots, \sigma^{m-d}(w)\}$$

forms a $GF(q^d)$-basis of $GF(q^m)$, i.e., a *normal basis of* $GF(q^m)$ 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

$$U(\sigma^d, f) := \{v \in GF(q^m, q^d, \sigma^d) \mid (f, v)_d = 0\} \tag{1.2}$$

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 cardinality $q^{d\,\deg(f)}$. Furthermore, the elements of $U(\sigma^d, f)$ are exactly the roots of

$$F_{q^d} := \sum_{i:=0}^{\deg(f)} f_i\, x^{q^{di}},$$

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. [6, (Lemma 3.69)] that

$$\Phi(q^d, f) = \prod_{i:=1}^{a} (q^{dk_i \deg(f_i)} - q^{d(k_i-1)\deg(f_i)}), \tag{1.3}$$

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

In this paper we start to investigate simultaneously the different module structures of $(GF(q^m), +)$ arising from the intermediate fields of the field extension $GF(q^m)$ over $GF(q)$. 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. We will see that different module structures can be studied with the aid of some basic properties of cyclotomic polynomials.

An element of $GF(q^m)$ over $GF(q)$ which is free with respect to any intermediate field of this field extension is called *completely free in* $GF(q^m)$ *over* $GF(q)$. The existence problem for completely free elements in arbitrary finite Galois extensions over any field was solved in Blessenohl and Johnsen [1]. In particular, concerning finite fields we have

THEOREM 1.1. (BLESSENOHL AND 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 $GF(q)$.*

The existence and nature of completely free elements seems to be very interesting in itself and because of the various applications of normal bases in practice (see Jungnickel [5, Chapters 3–5]). The main aim of this paper is to use the ideas developed in Section 2 to give a detailed, constructive and simpler proof of Theorem 1.1.

While the existence problem for completely free elements is easily reduced to the case where m is a prime power, the really difficult part is to settle the existence in this special case (see also [1]. For completeness and the convenience of the reader (especially since D. Blessenohl and K. Johnsen have published their results in German), we include a proof of the reduction of the existence problem to the special case (see Theorem 3.1).

If $m = r^n$ is a prime power ($n \geq 2$), i.e., if we are in the special case, using essentially our observations from Section 2, we will see that, fortunately, it is enough being able to handle simultaneously the *two* modules $GF(q^{r^n}, q, \sigma)$ and $GF(q^{r^n}, q^r, \sigma^r)$.

Altogether, our approach to the problem is based on some properties of cyclotomic polynomials, the structure of the unit groups of the rings of integers modulo n and on the fundamental Lemma 3.3 (concerning decompositions of the modules considered into direct sums of submodules) while D. Blessenohl and K. Johnsen in their (1986)-paper mainly use representation theory of finite abelian groups. Although their proof could slightly be condensed in Blessenohl [2], our approach is still simpler and seems to be more natural.

Furthermore, 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 on Orders of Elements Concerning Various Module Structures

In this section we study the additive group $(GF(q^m), +)$, simultaneously as a $GF(q)[x]$- and as a $GF(q^d)[x]$-module for some positive divisor d of m. We begin with a characterization of the $GF(q^d)[x]$-submodules of $(GF(q^m), +)$ which are invariant under the Frobenius automorphism σ.

THEOREM 2.1. *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 submodules $U(\sigma, f(x^d))$ of $GF(q^m, q, \sigma)$ and $U(\sigma^d, f)$ of $GF(q^m, q^d, \sigma^d)$ are equal as sets.

Conversely, if g is a monic divisor of $x^{m/d} - 1$ in $GF(q^d)[x]$ and if 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 coefficients in $GF(q)$ and f is equal to $g(x^d)$.

Proof. Let f be a monic divisor of $x^{m/d} - 1$ *in* $GF(q)[x]$. 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 $GF(q)$) and from (1.2).

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_{q^d} and F_q be the associated q^d-polynomial of g and the associated q-polynomial of f, respectively. G_{q^d} and F_q 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 they are equal. Therefore, g has coefficients in $GF(q)$ and $f = g(x^d)$. □

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 (normal bases generated by completely free elements), so that we have to consider elements which simultaneously generate both modules. We therefore next give an easy criterion to decide if v generates the module $U(\sigma^d, f)$, provided that v generates $U(\sigma, f(x^d))$.

Proposition 2.2. Let f be a monic divisor of $x^{m/d} - 1$ with coefficients in $GF(q)$. Let v be an element of $GF(q^m)$ with q-order $\mu(\sigma, v) = f(x^d)$. Then $\mu(\sigma^d, v)$, the q^d-order of v, is a monic divisor of f with coefficients in $GF(q^d)$.

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 an element of $GF(q^m)$ with q-order $f(x^d)$. As a consequence of Theorem 2.1, v is an element of $U(\sigma^d, f)$ and therefore $\mu(\sigma^d, v)$, the q^d-order of v, is a divisor of f. This is the first assertion.

One direction of the second assertion 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 and using the fact that $\mu(\sigma^d, v)$ divides f, we obtain

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

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 that f and $\mu(\sigma^d, v)$ are equal. □

We conclude this section with two applications of Proposition 2.2 which are very useful.

Corollary 2.3. Let v be free in $GF(q^m)$ over $GF(q)$ and let d be a positive divisor of m. Then v is free over $GF(q^d)$ if and only if the q^d-order of v has coefficients in $GF(q)$.□

Furthermore, we have

Theorem 2.4. *Let f be a monic divisor of $x^{m/d} - 1$ in $GF(q^d)[x]$. Assume that every irreducible divisor of f in $GF(q^d)[x]$ actually has coefficients in $GF(q)$. Then each element with q-order $f(x^d)$ 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. Completely Free Elements in Finite Fields

Let r be a prime number and $n \geq 1$ an integer. The main problem in the proof of Theorem 1.1 of Blessenohl and Johnsen is to settle the existence of completely free elements in $GF(q^{r^n})$ over $GF(q)$. This will be done constructively in this section. The general result then follows from Theorem 3.1, which reduces the existence problem to the special case where the degree of the extension is a prime power.

THEOREM 3.1. *Let m be a positive integer and let $\Pi_{i:=1}^{k} p_i^{a_i}$ be the prime power 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 $1 \leq i \leq k$, then $v := \Pi_{i:=1}^{k} v_i$ is completely free in $GF(q^m)$ over $GF(q)$.*

Proof. The proof proceeds in several steps.

Assume that $m = st$, where s and t are relatively prime, and let a and b be elements in $GF(q^m)$ such that $GF(q)(a)$ and $GF(q)(b)$, the intermediate fields of $GF(q^m)$ over $GF(q)$ obtained by adjoining a respectively b to the ground field $GF(q)$, are equal to $GF(q^s)$ and $GF(q^t)$, respectively. Then

$$GF(q^t)(a), \text{ the field generated by } GF(q^t) \text{ and } a, \text{ is equal to } GF(q^m) \qquad (3.1.1)$$

Proof. On one hand, $[GF(q^t)(a) : GF(q)]$, the degree of $GF(q^t)(a)$ over $GF(q)$, is equal to

$$[GF(q^t)(a) : GF(q^t)] \cdot [GF(q^t) : GF(q)] =: ut;$$

on the other hand, it is equal to

$$[GF(q^t)(a) : GF(q)(a)] \cdot [GF(q)(a) : GF(q)] =: vs$$

Since s and t are relatively prime and since $ut = vs$ divides $m = st$, we obtain $u = s$ and $v = t$, proving (3.1.1).

$$\text{If } a \text{ is free in } GF(q^s) \text{ over } GF(q), \text{ then } a \text{ is free in } GF(q^{st}) \text{ over } GF(q^t) \quad (3.1.2)$$

Proof. let ρ denote the restriction of σ, the Frobenius automorphism of $GF(q^m)$ over $GF(q)$, to the subfield $GF(q^s)$. Then ρ generates the Galois group of $GF(q^s)$ over $GF(q)$ which is cyclic of order s. By assumption we have that $N := \{a, \rho(a), \ldots, \rho^{s-1}(a)\}$ is a basis in $GF(q^s)$ over $GF(q)$. Since t and s are relatively prime, ρ^t, the restriction of σ^t to $GF(q^s)$, likewise generates the Galois group of $GF(q^s)$ over $GF(q)$. We therefore obtain $N = \{a, \rho^t(a), \ldots, \rho^{m-t}(a)\} = \{a, \sigma^t(a), \ldots, \sigma^{m-t}(a)\}$. So, it remains to show that N is a basis over $GF(q^t)$.

By (3.1.1) the $GF(q)$-basis $P := \{1, a, a^2, \ldots, a^{s-1}\}$ of $GF(q^s)$ is also a basis in $GF(q^m)$ over $GF(q^t)$. Let Λ be the unique (s, s)-matrix over $GF(q^t)$ defined by

$$\sigma^{jt}(a) = \sum_{i:=0}^{s-1} a^i \Lambda_{ij} \qquad \text{for } 0 \leq j \leq s - 1.$$

Then Λ describes a $GF(q^t)$-linear mapping from $GF(q^m)$ into itself. Since N is a basis of $GF(q^s)$ over $GF(q)$, we see that Λ actually has coefficients in $GF(q)$ and therefore describes also an $GF(q)$-linear automorphism of $GF(q^s)$. Therefore, Λ is invertible and thus N is a basis of $GF(q^m)$ over $GF(q^t)$, proving (3.1.2).

> If a is free in $GF(q^s)$ over $GF(q)$ and b is free in $GF(q^t)$ over $GF(q)$, then ab is free in $GF(q^m)$ over $GF(q)$. (3.1.3)

Proof. Let G, B and A be the Galois groups of $GF(q^m)$ over $GF(q)$, $GF(q^m)$ over $GF(q^s)$ and $GF(q^m)$ over $GF(q^t)$, respectively. Since s and t are relatively prime, A and B have trivial intersection while their complex product is equal to G. Let $w := \Sigma_{\gamma\in G}\lambda_\gamma\gamma(ab)$ be a linear combination of $N := \{\gamma(ab) \mid \gamma \in G\}$ over $GF(q)$. Then, as $a \in GF(q^s)$ and $b \in GF(q^t)$,

$$w = \sum_{\alpha\in A}\sum_{\beta\in B}\lambda_{\alpha\beta}(\alpha\beta)(ab) = \sum_{\alpha\in A}\left[\sum_{\beta\in B}\lambda_{\alpha\beta}\,\beta(b)\right]\alpha(a).$$

Now assume that w is equal to 0. Then, since a by (3.1.2) is free in $GF(q^m)$ over $GF(q^t)$, we have that $\Sigma_{\beta\in B}\,\lambda_{\alpha\beta}\beta(b) = 0$ for all α in A. By assumption, b is free in $GF(q^t)$ over $GF(q)$. Therefore, since the restriction of B on $GF(q^t)$ is the Galois group of $GF(q^t)$ over $GF(q)$, we have that $\lambda_{\alpha\beta} = 0$ for all α in A and all β in B showing that ab is free in $GF(q^m)$ over $GF(q)$, i.e., assertion (3.1.3).

> If a is completely free in $GF(q^s)$ over $GF(q)$ and b is completely free in $GF(q^t)$ over $GF(q)$, then ab is completely free in $GF(q^m)$ over $GF(q)$. (3.1.4)

Proof. Let r be a divisor of $m = st$. Since s and t are relatively prime, there exist divisors r_s and r_t of s and t, respectively such that $r = r_sr_t$. By assumption, a is free in $GF(q^s)$ over $GF(q^{r_s})$. Since r_t and sr_s^{-1} are relatively prime, an application of (3.1.1) and (3.1.2) shows that a is free in $GF(q^{sr_t})$ over $GF(q^{r_sr_t})$. Similar, since b is free in $GF(q^t)$ over $GF(q^{r_t})$ and since tr_t^{-1} and r_s are relatively prime, we have that b is free in $GF(q^{tr_s})$ over $GF(q^{r_sr_t})$. Finally, since sr_s^{-1} and tr_t^{-1} are relatively prime, an application of (3.1.3) shows that ab is free in $GF(q^m)$ over $GF(q^{r_sr_t}) = GF(q^r)$. This proves (3.1.4).

A simple induction on the number of different prime divisors of m finally completes the proof of Theorem 3.1. □

Throughout the rest of this section, we assume that $m = r^n$, where r is a prime number and $n \geq 2$ is an integer. We require some further notation.

Let $\Gamma(q, r^n)$ 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

$$\mu(\sigma^{r^i}, v) = x^{r^{n-i}} - 1 \quad \text{for } 0 \leq i \leq n-1 \tag{3.1}$$

Let $Q(r^i)$ denote the r^i-th cyclotomic polynomial and let $\Omega(q, r^n)$ be the number of elements v in $GF(q^{r^n})$ satisfying

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

Recall from Section 1 that the number of free elements in $GF(q^{r^n})$ over $GF(q)$ is denoted by $\Phi(q, x^{r^n} - 1)$.

We will separately handle the cases where r is equal to the characteristic of $GF(q)$ or not. The first one is rather simple.

THEOREM 3.2. *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, $\Gamma(q, r^n) = \Phi(q, x^{r^n} - 1) = q^{r^n - 1}(q-1)$.

Proof. Since r is the characteristic of $GF(q)$, we have that $x^{r^i} - 1 = (x - 1)^{r^i}$ for all nonnegative integers i. Hence this polynomial splits over $GF(q)$. Therefore, for every $0 \leq i \leq n - 1$ and every v in $GF(q^{r^n})$, the q^{r^i}-order of v has coefficients in $GF(q)$. The assertions follow now from Theorem 2.4 and (1.3). □

From now on we assume that r is different from the characteristic of $GF(q)$, in which case the polynomial $x^{r^n} - 1$ has no multiple roots over $GF(q)$. In order to give a fundamental characterization of the completely free elements in $GF(q^{r^n})$ over $GF(q)$ in Theorem 3.4, we repeatedly use a basic lemma which is well known in the more general setting of modules over a principle ideal domain (see [4, Section 3.9]). For the sake of completeness, we give a short proof.

LEMMA 3.3. Consider $(GF(q^m), +)$ as $GF(q)[x]$-module. Let f and g be monic divisors of $x^m - 1$ which are relatively prime. Let v be an element of the submodule $U(\sigma, fg)$. Then v can uniquely be written as $v_1 + v_2$, where $v_1 \in U(\sigma, f)$ and $v_2 \in U(\sigma, g)$.

Moreover, v generates $U(\sigma, fg)$ if and only if v_1 generates $U(\sigma, f)$ and v_2 generates $U(\sigma, g)$.

Proof. Since f and g are divisors of fg, the submodules $U(\sigma, f)$ and $U(\sigma, g)$ are contained in $U(\sigma, fg)$.

Since f and g are relatively prime, there exist polynomials a and b in $GF(q)[x]$ such that $af + bg = 1$. Assume that $v \in U(\sigma, f) \cap U(\sigma, g)$, then

$$v = (1, v)_1 = (af + bg, v)_1 = (a, (f, v)_1)_1 + (b, (g, v)_1)_1 = 0 + 0 = 0.$$

Hence, $U(\sigma, f)$ and $U(\sigma, g)$ have trivial intersection.

Now, let x and y be elements of q-order f and g, respectively, and let h be the q-order of $x + y$. Then $0 = (h, x + y)_1 = (h, x)_1 + (h, y)_1$ whence $(h, x)_1 = -(h, y)_1$ lies in $U(\sigma, f) \cap U(\sigma, g) = \{0\}$. Thus $(h, x)_1 = (h, y)_1 = 0$ which implies that f and g divide

h. Since f and g are relatively prime, fg divides h. Conversely, since $(fg, x + y)_1 = (g, (f, x)_1)_1 + (f, (g, y)_1)_1 = 0$, we obtain that h divides fg. As all polynomials involved are monic, we get that h is equal to fg.

Therefore, $x + y$ generates $U(\sigma, fg)$ and consequently, $U(\sigma, fg)$ is contained in the sum $U(\sigma, f) + U(\sigma, g)$.

Altogether we obtain that $U(\sigma, fg)$ is equal to the direct sum of $U(\sigma, f)$ and $U(\sigma, g)$. The truth of Lemma 3.3 now follows immediately. □

We are now able to give the proposed characterization of completely free elements in $GF(q^m)$ over $GF(q)$ which leads to a recursive formula for $\Gamma(q, r^n)$.

THEOREM 3.4. *Let $v \in GF(q^{r^n})$. Then there exist unique elements v_1 and v_2 in $GF(q^{r^n})$ such that $v = v_1 + v_2$,* the *q-order of v_1 divides $x^{r^{n-1}} - 1$ and the q-order of 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 (3.2).

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

Proof. Let $v \in GF(q^{r^n})$. Clearly, the q-order of v divides $x^{r^n} - 1$. 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, Lemma 3.3 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 $\mu(\sigma, v) = x^{r^n} - 1$ and therefore, by Lemma 3.3, $\mu(\sigma, v_1) = x^{r^{n-1}} - 1$ and $\mu(\sigma, v_2) = Q(r^n)$. Let $0 \le i \le n - 1$. As $x^{r^{n-1}} - 1 = (x^{r^i})^{r^{n-1-i}} - 1$ and $Q(r^n) = Q(r^{n-i})(x^{r^i})$ (see e.g. [6, Example 2.46] or [5, Theorem 2.6.2]), it follows from Proposition 2.2 that $\mu(\sigma^{r^i}, v_1)$ divides $x^{r^{n-1-i}} - 1$ and $\mu(\sigma^{r^i}, v_2)$ divides $Q(r^{n-i})$. As $\mu(\sigma^{r^i}, v) = x^{r^{n-i}} - 1$ by assumption, Lemma 3.3 implies that $\mu(\sigma^{r^i}, v_1) = x^{r^{n-1-i}} - 1$ and $\mu(\sigma^{r^i}, v_2) = Q(r^{n-i})$. Hence v_1 is completely free in $GF(q^{r^{n-1}})$ over $GF(q)$ while v_2 satisfies (3.2).

The converse likewise follows immediately using Lemma 3.3. Let v_1 be completely free in $GF(q^{r^{n-1}})$ over $GF(q)$ and assume that v_2 satisfies (3.2). 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 (3.1) and therefore is completely free in $GF(q^{r^n})$ over $GF(q)$. □

A recursive application of Theorem 3.4 gives

COROLLARY 3.5. Let v be a completely free element in $GF(q^{r^n})$ over $GF(q)$. Then v can uniquely be written as $\Sigma_{i:=0}^{n} v_i$, 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 $w_j = \Sigma_{i:=0}^{j} v_i$ is completely free in $GF(q^{r^j})$ over $GF(q)$.

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

Since $\Omega(q, r) = \Phi(q, Q(r))$ by definition, it remains to determine the numbers $\Omega(q, r^n)$ for $n \ge 2$. This will be done in what follows.

In order to handle the problem, we first have to understand the difficulties arising in turning from $GF(q)$ to $GF(q^r)$ as ground fields, i.e., in studying the *two* modules $GF(q^{r^n}, q, \sigma)$ and $GF(q^{r^n}, q^r, \sigma^r)$ simultaneously; otherwise, we will not be able to solve the global problem, i.e., the existence of elements satisfying (3.2). To this purpose, we consider elements in $GF(q^m)$ having q-order $Q(r^n)$ and q^r-order $Q(r^{n-1})$.

Observe that $Q(r^n) = Q(r^{n-1})(x^r)$ as $n \geq 2$, whence the modules $U(\sigma, Q(r^n))$ and $U(\sigma^r, Q(r^{n-1}))$ by Theorem 2.1 coincide as sets. Now the module structure of $U(\sigma, Q(r^n))$ depends on the factorization of $Q(r^n)$ over $GF(q)$ while the structure of $U(\sigma^r, Q(r^{n-1}))$ depends on the decomposition of $Q(r^{n-1})$ over $GF(q^r)$. This is the point where further properties of cyclotomic polynomials come into the game.

Let $h_1h_2 \ldots h_b$ be the complete factorization of $Q(r^{n-1})$ over $GF(q^r)$ and $f_1f_2 \ldots f_c$ the complete factorization of $Q(r^n)$ over $GF(q)$. Since q and r are relatively prime, the residue class $q + r^n \mathbb{Z}$ is a unit in the ring $\mathbb{Z}/r^n\mathbb{Z}$ of residues modulo r^n. Let $\text{ord}(r^n; q)$ denote the multiplicative order of $q + r^n\mathbb{Z}$ in $U(\mathbb{Z}/r^n\mathbb{Z})$, the group of units modulo r^n. The number $\text{ord}(r^{n-1}; q^r)$ is defined analogously. It is well known (see e.g., [6, Example 2.46] or [5, Corollary 1.5.9]) that

$$b = \varphi(r^{n-1})/\text{ord}(r^{n-1}; q^r) \quad \text{and} \quad \deg(h_i) = \text{ord}(r^{n-1}; q^r) \text{ for } 1 \leq i \leq b,$$
$$c = \varphi(r^n)/\text{ord}(r^n; q) \quad \text{and} \quad \deg(f_i) = \text{ord}(r^n; q) \text{ for } 1 \leq i \leq c. \tag{3.3}$$

As usual, φ denotes the Euler function, i.e., $\varphi(k)$ is the cardinality of $U(\mathbb{Z}/k\mathbb{Z})$.

We will see that the parameters in each of the decompositions only depend on the behavior of $q + r^n\mathbb{Z}$ in $U(\mathbb{Z}/r^n\mathbb{Z})$. Since $\varphi(r^n) = r^{n-1}(r - 1)$, the number $\text{ord}(r^n; q)$ has the form r^ks, where $0 \leq k \leq n - 1$ and s is a divisor of $r - 1$.

Next, recalling the content of Lemma 3.3 and Theorem 2.1, let $g_1g_2 \ldots g_a$ be the complete factorization of $Q(r^{n-1})$ over $GF(q)$. Then

$$a = \varphi(r^{n-1})/\text{ord}(r^{n-1}; q) \quad \text{and} \quad \deg(g_i) = \text{ord}(r^{n-1}; q) \text{ for } 1 \leq i \leq a. \tag{3.4}$$

Furthermore, $Q(r^n) = Q(r^{n-1})(x^r) = g_1(x^r)\, g_2(x^r) \ldots g_a(x^r)$. Any element w in $GF(q^{r^n})$ over $GF(q)$ of q-order $Q(r^n)$ and q^r-order $Q(r^{n-1})$ can uniquely be written as $\Sigma_{i:=1}^{a} w_i$ where $\mu(\sigma, w_i) = g_i(x^r)$ and $\mu(\sigma^r, w_i) = g_i$ for all $1 \leq i \leq a$. Therefore, for any i, we have to find the number of elements of q-order $g_i(x^r)$ and q^r-order g_i. It will turn out that these numbers are independent of the individual irreducible divisors of $Q(r^{n-1})$ over $GF(q)$.

Let g be any irreducible divisor of $Q(r^{n-1})$ over $GF(q)$. Before considering the *critical situation*, where g splits over $GF(q^r)$ and $g(x^r)$ splits over $GF(q)$, we concentrate on two cases which are easy to handle.

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 $\mu(\sigma, v) = g(x^r)$. Hence, any element of q^r-order g has q-order $g(x^r)$ and therefore the number of elements v in $GF(q^m)$ of q-order $g(x^r)$ and q^r-order g is equal to $\Phi(q^r, g)$. As a consequence, applying Lemma 3.3, we obtain that $\mu(\sigma^r, w) = Q(r^{n-1})$ implies $\mu(\sigma, w) = Q(r^n)$. We may therefore reduce the problem to a field extension of smaller prime power degree.

By (3.3) and (3.4), $g(x^r)$ is irreducible over $GF(q)$ if and only if

$$r\,\varphi(r^{n-1})/\mathrm{ord}(r^n;\, q) = \varphi(r^n)/\mathrm{ord}(r^n;\, q) = c = a = \varphi(r^{n-1})/\mathrm{ord}(r^{n-1};\, q),$$

i.e., if and only if

$$\mathrm{ord}(r^{n-1};\, q) = \mathrm{ord}(r^n;\, q)/r. \tag{3.5}$$

We conclude

THEOREM 3.6. *Let q be a prime power, r a prime number which does not divide q and let $n \geq 2$ be an integer. Assume that $ord(r^{n-1};\, q) = ord(r^n;\, q)/r$. Then*

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

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 $v \neq 0$ and therefore $\mu(\sigma^r, v) \neq 1$. Lemma 2.2 implies that $\mu(\sigma^r, v)$ divides g and therefore, by the irreducibility of g over $GF(q^r)$, we have that $\mu(\sigma^r, v) = g$. We obtain that any element of q-order $g(x^r)$ has q^r-order g whence the number of elements v of q-order $g(x^r)$ and q^r-order g is equal to $\Phi(q,\, g(x^r))$.

By (3.3) and (3.4), g is irreducible over $GF(q^r)$ if and only if

$$\varphi(r^{n-1})/\mathrm{ord}(r^{n-1};\, q) = a = b = \varphi(r^{n-1})/\mathrm{ord}(r^{n-1};\, q^r),$$

i.e., if and only if

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

and this is obviously satisfied if and only if

$$r \text{ does not divide the order of } q + r^{n-1}\mathbb{Z} \text{ in } U(\mathbb{Z}/r^{n-1}\mathbb{Z}). \tag{3.6$'$}$$

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

THEOREM 3.7. *Let q be a prime power, r a prime number which does not divide q and let $n \geq 2$ be an integer. Assume that r does not divide 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*

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

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

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 $j \geq 0$ and for all $1 \leq i \leq n - 1$, the order of q^{r^j} modulo r^i is equal to $\mathrm{ord}(r^i; q)$ and therefore likewise is not divisible by r. Consequently, 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 Theorem 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 main assertion.

The equation for $\Omega(q, r^n)$ follows, as this number is given by $\Gamma(q, r^n) = \Gamma(q, r^{n-1})\Omega(q, r^n)$ (see Theorem 3.4) and the fact that under the assumptions, $\Gamma(q, r^n) = \Phi(q, x^{r^n} - 1) = \Phi(q, x^{r^{n-1}} - 1)\Phi(q, Q(r^n))$ and $\Gamma(q, r^{n-1}) = \Phi(q, x^{r^{n-1}} - 1)$.

If $n = 2$, the assumption is always satisfied, since $\mathrm{ord}(r; q)$ divides $\varphi(r) = r - 1$ and therefore is not divisible by r. □

Next, we have to consider the

Critical Situation. Assume that neither $g(x^r)$ is irreducible in $GF(q)[x]$ nor g is irreducible in $GF(q^r)[x]$.

Then, since both polynomials split, several order-pairs $(\mu(\sigma, w), \mu(\sigma^r, w))$ may occur; the distribution of orders is not clear in advance.

We first determine explicitly the cases where the critical situation arises. It is easy to see that (3.5) is equivalent to:

> The subgroup of $U(\mathbb{Z}/r^n\mathbb{Z})$ generated by $q + r^n\mathbb{Z}$ contains the kernel of the natural epimorphism (3.5′)
>
> $$\eta : U(\mathbb{Z}/r^n\mathbb{Z}) \to U(\mathbb{Z}/r^{n-1}\mathbb{Z}),\ u + r^n\mathbb{Z} \to u + r^{n-1}\mathbb{Z}.$$

Together with (3.6′) this shows that we have to consider the group of units modulo $r^n\mathbb{Z}$ and its subgroup generated by $q + r^n\mathbb{Z}$. Using (3.3), (3.4), (3.5′) and (3.6′), one can show that, in the critical situation, $\mathrm{ord}(r^{n-1}; q) = \mathrm{ord}(r^n; q)$ and $\mathrm{ord}(r^{n-1}; q) = \mathrm{ord}(r^{n-1}; q^r)$ whence $g(x^r)$ over $GF(q)$ splits into the product of r irreducible polynomials and g over $GF(q^r)$ splits into the product of r irreducible polynomials.

The structure of the unit groups is well known; a proof of the following theorem may be found in Ireland and Rosen [3, Chap. 4].

THEOREM 3.8. *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 the direct product of the cyclic subgroups $<5 + 2^n\mathbb{Z}>$ and $<-1 + 2^n\mathbb{Z}>$ of order 2^{n-2} and 2, respectively, provided that $n \geq 3$.*

Recall that $\mathrm{ord}(r^n; q)$ is of the form $r^k s$, where $0 \leq k \leq n - 1$ and where s is a divisor of $r - 1$.

The kernel of η (see (3.5′)) is equal to $<1 + r^{n-1} + r^n\mathbb{Z}>$ and has order r. Hence a necessary condition for (3.5′) is that r divides $\mathrm{ord}(r^n; q)$. Let us therefore assume that the parameter k is at least 1. It is obvious that (3.5′) 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 η.

By Theorem 3.8, let therefore $n \geq 3$ and $r = 2$. In this case, the kernel of η is equal to $< 5^{2^{n-3}} + 2^n\mathbb{Z} >$ and has order 2. Consequently, if ord(2^n; q) is divisible by 4, it is the unique subgroup of order 2 of $U(\mathbb{Z}/2^n\mathbb{Z})^2 = \{x^2 + 2^n\mathbb{Z} \mid x \in \mathbb{Z}, x \text{ odd}\}$ and therefore the subgroup $< q + 2^n\mathbb{Z} >$ likewise contains the kernel of η. Hence (3.5′) holds, provided that $k \geq 2$. Trivially, if ord(2^n; q) $= 2$ and $q \equiv 5^{2^{n-3}} \bmod 2^n$, then $< q + 2^n\mathbb{Z} >$ contains the kernel of η.

Altogether we conclude that (3.5′) does not hold if and only if $k = 0$ or ($r = 2$, $k = 1$, $n \geq 3$ and $q \not\equiv 5^{2^{n-3}} \bmod 2^n$). The latter case is called the *exceptional case* in [5].

If $k = 0$ then ord(r^n; q) $=$ ord(r^{n-1}; q) $=$ ord(r^{n-1}; q^r) and we have Case II which is covered by Theorem 3.7.

Summarizing, we have the pleasant result that the critical situation only occurs in the exceptional case.

In the following theorem the exceptional case is handled.

THEOREM 3.9. *Assume the exceptional case. Let* $v \in GF(q^{2^n})$. *Then* v *satisfies* (3.2) *if and only if it has q-order* $Q(2^n)$ *and* q^2*-order* $Q(2^{n-1})$.

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 $n \geq 3$ and let furthermore $q \neq 5^{2^{n-3}} \bmod 2^n$. Then, over $GF(q)$, the polynomial $Q(2^{n-1})$ splits into the product of 2^{n-3} irreducible factors each of degree 2. 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 Theorem 2.4 shows that any free element in $GF(q^{2^n})$ over $GF(q^2)$ is completely free over $GF(q^2)$. Together with Theorem 3.7 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.

Let g be any irreducible divisor of $Q(2^{n-1})$ over $GF(q)$. Then $g(x^2)$ divides $Q(2^n)$ 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. 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 α is not equal to 0. Therefore, $\sigma(v) = \upsilon v$, where $\upsilon := (\zeta - \beta)/\alpha \in GF(q^2) - GF(q)$. Now

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

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

We conclude that any element v with $\deg(\mu(\sigma^2, v)) = 1$ has q-order $g(x^2)$. Now, using (1.3), we obtain

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

This number is greater than 0 and independent of the choice of g, wherefore, together with Lemma 3.3, the first statement of the theorem and the fact that $Q(2^{n-1})$ over $GF(q)$ splits into 2^{n-3} irreducible factors, we obtain that

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

i.e., the second assertion. □

Altogether, this completes our investigation of elements in $GF(q^m)$ having q-order $Q(r^n)$ and q^r-order $Q(r^{n-1})$ and by Theorem 3.4 we are now able to handle simultaneously the two module structures $GF(q^{r^n}, \sigma, q)$ and $GF(q^{r^n}, \sigma^r, q^r)$.

Furthermore, because of the nature of Theorems 3.6, 3.7 and 3.9 we also obtain a recursive formula for the number of elements in $GF(q^{r^n})$ satisfying (3.2) and, again using Theorem 3.4 and its Corollary 3.5, we have even settled the existence of completely free elements in $GF(q^{r^n})$ over $GF(q)$, as desired.

In the following main theorem on completely free elements in $GF(q^{r^n})$ over $GF(q)$ we summarize the results so far obtained.

THEOREM 3.10. *Let q be a prime power, r a prime number different from the characteristic of $GF(q)$ and $n \geq 1$ an integer.*

Moreover, let the nonnegative integers k and s be defined by $ord(r^n; q) = r^k s$, where s is a divisor of $r - 1$ and $ord(r^n; q)$ denotes the order of q modulo r^n. Let $t := \max \{a \mid a$ an integer and $a \leq k/2\}$.

For $1 \leq j \leq n$ let $\Gamma(q, r^j)$ be the number of completely free elements in $GF(q^{r^j})$ over $GF(q)$. For $1 \leq j \leq n$, let $\Omega(q, r^j)$ denote the number of elements in $GF(q^{r^j})$ over $GF(q)$ having q^{r^i}-order $Q(r^{j-i})$ for all $0 \leq i \leq j - 1$ (with $Q(r^{j-i})$ being the r^{j-i}th cyclotomic polynomial). Then

(i) *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 has q^{r^i}-order $Q(r^{n-i})$ for all $0 \leq i \leq n - 1$. Furthermore,*

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

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

(iii) *If $k = 0$ or ($k = 1$ and r is odd) or ($n \geq 3$, $k = 1$, $r = 2$ and $q \equiv 5^{2^{n-3}}$ mod 2^n), then any free element in $GF(q^{r^n})$ over $GF(q)$ is completely free in $GF(q^{r^n})$ over $GF(q)$.*

(iv) *If ($n \geq 3$, $k = 1$, $r = 2$ and ($q \equiv -1$ mod 2^n or $q \equiv -5^{2^{n-3}}$ mod 2^n)), then*

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

(v) *If $k \geq 2$ then*

$$\Omega(q, r^n) = (q^{sr^{k-t}} - 1)^{(r-1)r^{n-k+t-1}/s}.$$

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

Proof. The only assertion left to prove is (v). Let $k \geq 2$, then necessarily $n \geq 3$.

By Theorem 3.6 we have $\Omega(q, r^n) = \Omega(q^r, r^{n-1})$. In order to apply the recursion, we have to determine the order of q^r modulo r^{n-1}. By Theorem 3.8, in either case, the subgroup of $U(\mathbb{Z}/r^n\mathbb{Z})$ generated by $q + r^n\mathbb{Z}$ contains the kernel of $\eta : \mathbb{Z}/r^n\mathbb{Z} \to \mathbb{Z}/r^{n-1}\mathbb{Z}$, $x + r^n\mathbb{Z} \to x + r^{n-1}\mathbb{Z}$ (see (3.5')). We obtain that $\mathrm{ord}(r^{n-1}; q) = r^{k-1}s$. Since this number is divisible by r, we obtain furthermore that $\mathrm{ord}(r^{n-1}; q^r) = r^{k-2}s$.

What we have to consider now is whether we meet the exceptional case in starting with the assumptions in (v). Therefore, assume that $r = 2$ and that $\mathrm{ord}(2^n; q)$ is divisible by 4. Using Theorem 3.8 we get that $U(\mathbb{Z}/2^n\mathbb{Z})^2 = <5^2 + 2^n\mathbb{Z}>$ contains $q^2 + 2^n\mathbb{Z}$. Applying η, we see that $<q^2 + 2^{n-1}\mathbb{Z}>$ is a subgroup of $<5^2 + 2^{n-1}\mathbb{Z}> = U(\mathbb{Z}/2^{n-1}\mathbb{Z})^2$ and therefore contains the kernel of $\gamma: U(\mathbb{Z}/2^{n-1}\mathbb{Z}) \to U(\mathbb{Z}/2^{n-2}\mathbb{Z})$, $x + 2^{n-1}\mathbb{Z} \to x + 2^{n-2}\mathbb{Z}$. An induction argument shows finally that under the assumption $k \geq 2$, the exceptional case will never occur in the recursion.

By the definition of the parameter t, applying the recursion t times, we obtain that

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

and, after turning from $GF(q)$ to $GF(q^{r^t})$, Case II holds, whence Theorem 3.7 implies that

$$\Omega(q^{r^t}, r^{n-t}) = \Phi(q^{r^t}, Q(r^{n-t})).$$

Using (1.3), after some simplifications, we see that this number is equal to the one given in assertion (v), concluding the proof. □

In our final example, we consider field extensions of degree r^3, i.e., the smallest nontrivial example.

EXAMPLE 3.11. We want to determine the number of completely free elements in $GF(q^m)$ over $GF(q)$, where $m = r^3$ is a cube of a prime number r which does not divide q.

We consider the case $r = 2$ first.

If $q \equiv 1 \bmod 8$ or $q \equiv 5 \bmod 8$, then $\Omega(q, 8) = \Phi(q, Q(8))$ and $\Gamma(q, 8) = \Phi(q, x^8 - 1)$, i.e., any free element in $GF(q^8)$ over $GF(q)$ is completely free in $GF(q^8)$ over $GF(q)$. Using (1.3), 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 3.9. Using recursion, in both cases we get that $\Gamma(q, 8) = (q - 1)^2(q^2 - 1)(q^4 - 4q^2 + 3)$. In comparison with $\Phi(q, x^8 - 1) = (q - 1)^2(q^2 - 1)^3$, 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 $GF(3)$.

Finally, let r be odd.

Let $r^k s$ be the order of q modulo $r^3\mathbb{Z}$, where s is a divisor of $r - 1$. Then $k \leq 2$.

If $k \leq 1$ then any free element in $GF(q^{r^3})$ over $GF(q)$ is completely free in $GF(q^{r^3})$ over $GF(q)$ and therefore

$$\Gamma(q, r^3) = \Phi(q, x^{r^3} - 1).$$

If $k = 2$, then

$$\begin{aligned}\Gamma(q, r^3) &= \Gamma(q, r^2)\, \Omega(q, r^3)\\ &= \Phi(q, x^{r^2} - 1)\Phi(q^r, Q(r^2)).\end{aligned}$$ □

References

1. Blessenohl, D. and Johnsen, K., Eine Verschärfung des Satzes von der Normalbasis, *J. of Algebra 103*, (1986), pp. 141–159.
2. Blessenohl, D., Supplement to "Eine Verschärfung des Satzes von der Normalbasis," *J. of Algebra 132*, (1990), pp. 154–159.
3. Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory*, Springer, New York, (1982).
4. Jacobson, N., *Basic Algebra I*. 2nd Ed., Freeman and Company, New York, (1985).
5. Jungnickel, D., *Finite Fields. Structure and Arithmetic.* Bibliographisches Institut, Mannheim, (1993).
6. Lidl, R. and Niederreiter, H., *Finite Fields*. Addison-Wesley, Reading, Massachusetts, (1983).

INSTRUCTIONS FOR AUTHORS

Authors are encouraged to submit high quality, original work which has neither appeared in, nor is under consideration by, other journals.

Authors should submit five hard copies of their final manuscript to: Karen Cullen, Editorial Office, Kluwer Academic Publishers, 101 Philip Drive, Norwell, MA 02061 Tel. 617-871-6300; FAX: 617-871-6528

For prompt attention, all correspondence can be directed to this address. Enclose with each manuscript on a separate page, from three to five key words.

Enclose originals for the illustrations, for one copy of the manuscript. Photocopies of the figures may accompany the remaining copies of the manuscript. Alternatively, original illustrations may be submitted after the paper has been accepted.

Enclose a separate page giving the complete preferred mailing address of the contact author for correspondence and return of proofs. Please include a telephone number, fax number and e-mail address.

The refereeing is done by anonymous reviewers.

All papers should be written in English.

Authors are encouraged to send for detailed **Instructions for Authors** in which the preferred style of the manuscript is outlined.

The following **1993 Journals Catalogues** are available:

* **Journals in Natural and Applied Sciences**
(including among others the areas: Applied Mechanics,
Electrical Engineering, Mathematics)
* **Journals in Electrical Engineering**
* **Journals in Computer and Information Science**

ORDER FORM

Designs, Codes and Cryptography - An International Journal, **ISSN 0925-1022**

□ Please enter ___ 1993 Subscription(s), Dfl.397.00/US$248.00 incl. p&h
□ Please enter ___ 1993 Private subscription(s), Dfl.205.00/US$85.00 incl. p&h
(by signing the form, private subscribers are declaring that the subscription is for their personal use only)
□ Please send a **Free Sample Copy**
□ Please send the 1993 Journals Catalogue(s) on:
□ Natural and Applied Sciences □ Electrical Engineering □ Computer and Information Science

Payment can be made by credit card, bank draft, personal cheque or international money order. US$-prices apply to deliveries in USA, Canada, and Mexico only. Orders within The Netherlands are subject to the addition of 6% VAT (BTW). Prices are subject to change without notice.

□ Payment enclosed to the amount of ______________ □ Please invoice me/my institution/company
□ Please charge my credit card account:

Card No. |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

□ Access □ American Express □ MasterCard
□ Diners Club □ Eurocard □ Visa Expiry date:____________

NAME:______________________________

POSITION:______________________________

ADDRESS:______________________________

CITY:______________ STATE:______________

COUNTRY:______________ POSTAL CODE:______________

SIGNATURE:______________ DATE:______________

Please fill in the order form and send to your supplier, or to:

Kluwer Academic Publishers
P.O. Box 322
3300 AH Dordrecht
The Netherlands
☎ (0)78-524400
Fax (0)78-524474

Customers in USA, Canada. and Mexico
Kluwer Academic Publishers
P.O. Box 358, Accord Station
Hingham, MA 02018-0358
U.S.A.
☎ (617)871-6600
Fax (617)871-6528