Glasgow Math. J. **43** (2001) 383–398.

PRIMITIVE COMPLETE NORMAL BASES FOR REGULAR EXTENSIONS

DIRK HACHENBERGER

Institut für Mathematik der Universität Augsburg, D-86135 Augsburg, Germany
e-mail: hachenberger@math.uni-augsburg.de

(Received 20 December, 1999)

Abstract. The extension E of degree n over the Galois field $F = \mathrm{GF}(q)$ is called *regular over* F, if $\mathrm{ord}_r(q)$ and n have greatest common divisor 1 for all prime divisors r of n which are different from the characteristic p of F (here, $\mathrm{ord}_r(q)$ denotes the multiplicative order of q modulo r). Under the assumption that E is regular over F and that $q-1$ is divisible by 4 if q is odd and n is even, we prove the existence of a primitive element $w \in E$ which is also completely normal over F (the latter means that w simultaneously generates a normal basis for E over *every* intermediate field K of E/F). Our result achieves, for the class of extensions under consideration, a common generalization of the theorem of Lenstra and Schoof on the existence of primitive normal bases [**12**] and the theorem of Blessenohl and Johnsen on the existence of complete normal bases [**1**].

1991 *Mathematics Subject Classification*. 11T30, 12E20, 11T24.

1. The main result. The famous normal basis theorem states that for every (finite dimensional) Galois extension E/F there exists an element w in E whose set of conjugates under the Galois group G constitutes a basis of E as F-vector space. Equivalently, the additive group $(E,+)$ of E is free on one generator when considered as a module over the group algebra FG. Each generator is called a *normal* or a *free element of* E *over* F.[1] For arbitrary finite fields E and F the normal basis theorem was first proved by Hensel [**10**] in 1888; for infinite fields the result is due to Noether [**16**].

In the present paper we are concerned with finite fields. So, let $F = \mathrm{GF}(q)$ be the Galois field with q elements and let E be the extension of degree n over F. Then the Galois group G is cyclic and admits the Frobenius automorphism σ_F (mapping $u \in E$ to u^q) as a canonical generator. Consequently, the FG-action on $(E,+)$ can be described in terms of the (univariate) polynomial ring $F[x]$ over F by defining the scalar multiplication

$$f \circ_F w := f(\sigma_F)(w), \quad f \in F[x], \ w \in E, \tag{1.1}$$

i.e., by evaluating the polynomial f at the Frobenius automorphism and by applying the resulting F-endomorphism $f(\sigma_F)$ of E to w. We call E an $F[x]$-*module*. The F-*order* (or q-*order*) of $w \in E$ is defined to be the monic polynomial $\mu \in F[x]$ of least

[1]Unfortunately, the terminology is not consistent. We have used the term *free* in [**7**] and several other papers. This time, as in [**14**], we shall use the term *normal*.

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

degree such that $\mu \circ_F w = 0$; it is denoted by $\mathrm{Ord}_F(w)$ (or also by $\mathrm{Ord}_q(w)$). It is well known (see e.g. [7, Section 1]) that $w \in E$ is normal over F if and only if $\mathrm{Ord}_F(w) = x^n - 1$, i.e., if and only if $\mathrm{Ord}_F(w)$ is equal to the minimal polynomial of E when considered as $F[x]$-module.

For every divisor k of n there exists exactly one subfield K of E which has degree k over F. If H is the Galois group of E over K, then $(E, +)$ likewise is free on one generator as KH-module, and using the Frobenius automorphism $\sigma_K = \sigma_F^k$ of E/K, the KH-action is described via the polynomial ring $K[x]$ by

$$g \circ_K w := g(\sigma_K)(w), \quad g \in K[x], \ w \in E. \tag{1.2}$$

Analogously, we define the *K-order* (or *q^k-order*) *of* $w \in E$ to be the monic polynomial $v \in K[x]$ of least degree such that $v \circ_K w = 0$. Since the degree of E over K is equal to n/k, w is normal in E over K if and only if $\mathrm{Ord}_K(w) = x^{n/k} - 1$, the latter is the minimal polynomial of E when considered as a $K[x]$-module.

Now, it might happen that, for some intermediate field K, a normal element for E over F is not normal over K. For example, if $\eta \in \mathrm{GF}(64)$ is a primitive 9th root of unity, then $\eta + \eta^3$ is normal in GF(64) over GF(2) but not over GF(4), as

$$\mathrm{Ord}_4(\eta + \eta^3) = x^2 + \eta^6 x + \eta^3 \neq x^3 - 1.$$

The *strengthening of the normal basis theorem*, however, which is due to Blessenohl and Johnsen [1], states that for *every* finite extension E over *any* finite field F there exists an element w which simultaneously is normal over K for *every* intermediate field K of E/F. Such an element is called *completely normal* or *completely free* in E over F. (As was first proved by Faith [6] in 1957, see also [1], this *complete normal basis theorem* also holds for (finite dimensional) Galois extensions over infinite fields.)

For finite fields there is another 'strengthening of the normal basis theorem', namely the *primitive normal basis theorem* of Lenstra and Schoof, which simultaneously concerns the multiplicative and the additive group of the extension field E. Recall that the multiplicative group E^* of E is cyclic, i.e., free on one generator as a module over the ring of integers; an element w of E is called *primitive*, if w is a generator of E^*. Now the theorem of Lenstra and Schoof states that for every finite extension E over a finite field F there exists a primitive element in E which additionally is normal over F. The following example shall indicate that the existence of such an element is non-trivial. Consider $E = \mathrm{GF}(64)$ over $F = \mathrm{GF}(2)$: the roots of $x^6 + x^5 + x^4 + x^2 + 1$ are normal for E over F, but not primitive; the roots of $x^6 + x + 1$ are primitive but not normal; the roots of $x^6 + x^5 + 1$ are primitive and normal for E over F.

The two stronger versions of the normal basis theorem immediately lead to the following problem, which concerns a common generalization of the theorem of Lenstra and Schoof and the theorem of Blessenohl and Johnsen.

PROBLEM 1.1. *Let E be a finite extension over a finite field F. Does there exist a primitive element in E which is completely normal over F?*

Consider again $E = \mathrm{GF}(64)$ over $F = \mathrm{GF}(2)$: the roots of $x^6 + x^5 + 1$ are primitive but not completely normal for E over F. If v is a root of $x^6 + x^5 + x^4 + x^2 + 1$ then v is completely normal for E over F, but v is not primitive. However, there are

exactly six elements in E which are primitive and completely normal over F, and these are precisely the roots of the polynomial $x^6 + x^5 + x^4 + x + 1$.

The following conjecture is due to Morgan and Mullen [**14**] (see also [**15**, Conjecture 9]).

CONJECTURE 1.2. *For every prime power $q > 1$ and every integer $n \geq 1$ there exists a primitive element $w \in E = \mathrm{GF}(q^n)$ which is completely normal over $F = \mathrm{GF}(q)$.*

By means of a computer search, Morgan and Mullen [**14**] have supported their conjecture by calculating for every pair (q, n), with $q \leq 97$ a prime and $q^n < 10^{50}$, a monic irreducible polynomial $\mu_{q,n}$ of degree n over $\mathrm{GF}(q)$ whose roots are primitive and completely normal for $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$. Besides an extensive table with 1061 polynomials they have also determined the exact number of primitive completely normal elements for the 56 pairs (q, n), where $q = 2, 3, 4, 5, 7, 8, 9$ and $n \leq 18, 12, 9, 8, 6, 5, 5$, respectively.

In the present paper we shall confirm Conjecture 1.2 by proving the *primitive complete normal basis theorem* for a considerably large class of extensions (see Theorem 1.4). We require a definition.

DEFINITION 1.3. The field $E = \mathrm{GF}(q^n)$ is called *regular over* $F = \mathrm{GF}(q)$ if for every prime divisor r of n which is different from the characteristic of F, $\mathrm{ord}_r(q)$ and n are relatively prime, where $\mathrm{ord}_r(q)$ denotes the smallest integer $k \geq 1$ such that $q^k - 1$ is divisible by r (i.e., the multiplicative order of q modulo r). The pair (q, n) is likewise called *regular*.

Let p be the characteristic of $\mathrm{GF}(q)$ and write $n = m\pi$, where π is a power of p and m is prime to p. It is easy to see that (q, n) is regular if and only if n and $\mathrm{ord}_{\nu(m)}(q)$ are relatively prime, where $\nu(m)$ denotes the square-free part of m. (Of course, (q, n) is regular if and only if (q, k) is regular for every divisor k of n.)

Our main result is the following theorem.

THEOREM 1.4. *Let E be the field extension of degree n over a finite field $F = \mathrm{GF}(q)$. Assume that E is regular over F. Assume further that $q - 1$ is divisible by 4 if q is odd and n is even. Then there exists a primitive element $w \in E$ which is completely normal over F.*

We close this section with some examples for regularity which also indicate that the class of extensions satisfying the assertion of Theorem 1.4 is in fact considerably large.

1. If n is the power of a prime r, then (n, q) is regular for each prime power $q > 1$.
2. If q is given and $n = m\pi$ is as above, then (n, q) is regular if $\nu(m)$ divides $q - 1$.
3. A *Carmichael number* is an odd composite integer $N \geq 1$ such that $r - 1$ divides $N - 1$ for every prime divisor r of N (see [**11**, p. 128]; there exist infinitely many Carmichael numbers). E.g., 561, 1105, 1729 and 2465 are Carmichael numbers. Now, if N is any Carmichael number, then (N^s, q) is regular for each prime power $q > 1$ and each integer $s \geq 1$.
4. If $q \geq 2$ is any prime power and if all primes in n lie in the set $L := \{7, 11, 13, 17, 19, 31, 41, 47, 59, 61, 73, 97, 101, 107, 109, 139, 151, 163, 167, 173, 179, 181,$

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

193 } (no matter in which multiplicity the primes occur in n), then $\mathrm{GF}(q^n)$ is regular over $\mathrm{GF}(q)$. (The set L above has been determined as follows: we have started with $L = \{7\}$ and considered all primes r with $8 \leq r \leq B = 200$ in increasing order; if s is not a divisor of $r - 1$ for every s in the current set L, then r is added to L. When taking $B = 1000$, one obtains a list of 70 primes (the total number of primes r with $7 \leq r \leq 1000$ is equal to 165); when taking $B = 100000$ one obtains a list with 3181 primes the largest of which is 99907 (the total number of primes in the interval [7, 100000] is equal to 9585).)

2. Outline. The notion of regularity was introduced in [**7**] while studying the structure of completely normal elements for finite fields. So, [**7**] is the standard reference for the theory of (complete) normal bases for finite fields. For the general background on the theory and applications of finite fields, the reader may consult Lidl and Niederreiter [**13**].

In Section 3 and Section 4 we summarize some facts from [**7**] on the nature of completely normal elements for the class of *completely basic* and the class of regular extensions, respectively. The main result in this respect is Theorem 4.3, which gives a characterization of the *complete generators* for *regular cyclotomic modules*.

In order to combine primitivity and (complete) normality we use the theory of Gauss and character sums. The idea of applying these methods to study primitivity in combination with normality has its origins in papers of Carlitz [**3**] and Davenport [**5**], who first investigated the existence of primitive normal bases. In Section 5, for extensions as considered in Theorem 1.4, we derive a sufficient criterion for the existence of a primitive element which additionally is completely normal, and finally, through analysing this criterion, the proof of Theorem 1.4 is completed in Section 6. In Section 7 we shall conclude with some remarks concerning Problem 1.1 in its full generality.

The reader will have observed that, in Theorem 1.4, besides regularity, we have assumed that $q - 1$ is divisible by 4 if q is odd and n is even. This assumption is necessary to exclude, among the regular extensions, the subclass of *exceptional extensions* (see also Definition 20.2 in [**7**]). These do not allow the characterization of completely normal elements which is based on Theorem 4.3.

Definition 2.1. Let $q > 1$ be a prime power and $n \geq 1$ an integer. Assume that (q, n) is regular. Let n_2 be the largest power of 2 dividing n. Then the pair (q, n) as well as the extension $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$ are called *exceptional* provided the following conditions are satisfied: q is odd, $n_2 \geq 8$, $\mathrm{ord}_{n_2}(q) = 2$, and $q - 1 - \frac{1}{2}n_2$ is not divisible by n_2.

3. Completely basic extensions. The study of normality under variations of the ground field goes back to the work of Faith [**6**]. He has defined a Galois extension E/F to be *completely basic* if each normal element of E over F already is completely normal. Hence, in the context of finite fields, a trivial application of the theorem of Lenstra and Schoof shows that primitive completely normal elements do exist for completely basic extensions. In the present section we will therefore compare the classes of completely basic and regular extensions. The outcome is that every completely basic extension is regular although the regular class is much larger than the complete basic one.

One of the main results in [**6**] is that Kummer extensions are completely basic. Motivated by the work of Faith, Blessenohl and Johnsen [**2**] have characterized the completely basic extensions among the abelian extensions. For the case of finite fields, an elementary proof of that characterization is given in [**7**, Theorem 15.7]. It is as follows, where now, for an integer k, k' denotes the largest divisor of k which is prime to the characteristic p of the underlying fields.

THEOREM 3.1. *Let E be the field extension of degree n over $F = \mathrm{GF}(q)$. Then the following statements are equivalent.*

1. *E is completely basic over F.*
2. *If w is any normal element for E over F and if r is any prime divisor of n, then w is normal for E over $\mathrm{GF}(q^r)$.*
3. *For every prime divisor r of n, the multiplicative order of q modulo $(\frac{n}{r})'$ is not divisible by r.*

For example, if n is a power of the characteristic p of $F = \mathrm{GF}(q)$, then (q, n) is completely basic (which means that $\mathrm{GF}(q^n)$ is completely basic over $\mathrm{GF}(q)$). Or, if $n = r^2$ is the square of a prime r, then (q, n) is completely basic (see [**7**, Corollary 15.6]). Also, if n divides $q - 1$, then (q, n) is completely basic.

The following result relies on Definition 1.3 and Theorem 3.1.

PROPOSITION 3.2. *Assume that (q, n) is completely basic. Then (q, n) is also regular.*

Proof. Let $n = m\pi$, where $m = n'$ and π is a power of the characteristic p. If p does not divide $\mathrm{ord}_m(q)$ then it does not divide $\mathrm{ord}_{v(m)}(q)$.

Next, let r be a prime divisor of m and write $m = \rho k$, where ρ is a power of r and k is prime to r. The multiplicative order of q modulo m/r is equal to the least common multiple a of $\mathrm{ord}_{\rho/r}(q)$ and $\mathrm{ord}_k(q)$. The least common multiple b of $\mathrm{ord}_r(q)$ and $\mathrm{ord}_{v(k)}(q)$ is equal to $\mathrm{ord}_{v(m)}(q)$. By assumption, r does not divide a. If r^2 divides ρ, then b divides a, whence r is prime to b. If $r = \rho$, then $a = \mathrm{ord}_k(q)$ which is divisible by $\mathrm{ord}_{v(k)}(q)$. Since $\mathrm{ord}_r(q)$ divides $r - 1$, we have again that r is prime to b. Hence, a completely basic pair is also regular. □

We shall see soon that the class of regular extensions is much larger than the class of completely basic extensions. For this purpose, with m being as in the proof of Proposition 3.2, observe first that the multiplicative order of q modulo m has the form

$$\mathrm{ord}_m(q) = \mathrm{ord}_{v(m)}(q) \cdot \prod_r r^{\alpha(r)}, \tag{3.1}$$

where the product runs over all prime divisors r of m and where $\alpha(r) \geq 0$. Moreover, if for a prime divisor r of m, m_r is the maximal power of r dividing m, then

$$\mathrm{ord}_{m_r}(q) = \mathrm{ord}_r(q) \cdot r^{\alpha(r)}, \tag{3.2}$$

and therefore $r^{\alpha(r)}$ divides m_r/r. Now, if $\alpha(r) \geq 2$, then

$$\mathrm{ord}_{m_r/r}(q) = \frac{\mathrm{ord}_{m_r}(r)}{r} \tag{3.3}$$

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

is divisible by r. Consequently, if (q, n) is completely basic, then $\alpha(r) \leq 1$ for all prime divisors r of m. Moreover, by [7, Lemma 20.4], the following is true.

PROPOSITION 3.3. *Assume that (q, n) is a regular pair. Then the following assertions are equivalent.*

1. *(q, n) is not exceptional and $\alpha(r) \leq 1$ for each prime divisor r of m.*
2. *(q, n) is completely basic.*

Now, if Γ is a finite set of prime numbers, then let $\nu(\Gamma)$ be the product of all $s \in \Gamma$. Moreover, let $N(\Gamma)$ be the set of integers $k \geq 1$ such that $\nu(k)$ divides $\nu(\Gamma)$. Assuming that $(q, \nu(\Gamma))$ is completely basic, we have that $(q, \nu(\Gamma))$ is regular by Proposition 3.2. However, by Proposition 3.3 and (3.1), the set of integers $n \in N(\Gamma)$ such that (q, n) is completely basic is *finite*, whereas (q, n) is regular for *all* $n \in N(\Gamma)$. This is because the α-values (see (3.1) and (3.2)) can become arbitrarily large without effecting the regularity: regularity is a *local* condition in the sense that it involves only the square-free part of an integer.

We finally mention that, by Proposition 3.3, (q, n) is completely basic if (q, n) is regular and $m/\nu(m)$ is square-free (where again $m = n'$). Moreover, we have the following lemma, which will be used in Section 6.

LEMMA 3.4. *Assume that (q, n) is regular but not completely basic. Then $m = n'$ is divisible by the cube r^3 of a prime r. Moreover, if m is even, if $q - 1$ is divisible by 4 and if m is not divisible by the cube of an odd prime, then 16 divides m.*

4. Complete normality for regular extensions. In the present section, we summarize the essential properties of completely normal elements for regular extensions. For the proofs, we refer to [7].

Throughout, let again p be the characteristic of $F = \mathrm{GF}(q)$ and write $n = m\pi$ where m is not divisible by p and π is a power of p. Let $E = \mathrm{GF}(q^n)$ and let σ_F, as in Section 1, denote the Frobenius automorphism over F. Moreover, for a divisor k of m, let Φ_k be the kth cyclotomic polynomial over F.

The subset

$$U_k := U_{F,\Phi_k^\pi} = \{w \in E \mid \Phi_k^\pi \circ_F w = 0\} \tag{4.1}$$

of E is a σ_F-invariant F-subspace, whence we call U_k a *cyclotomic module* over F. Next, we define F_k to be the subfield of all $\lambda \in E$ such that $\lambda U_k \subseteq U_k$, i.e., F_k is the largest subfield of E such that U_k is an F_k-vector space. Then the degree $[F_k : F]$ of F_k over F is equal to

$$\kappa(k) := \frac{k\pi}{\nu(k)}. \tag{4.2}$$

(The latter is proved in Section 18 of [7] for a more general class of σ_F-invariant F-subspaces of an algebraic closure of F.) The value $\kappa(k)$ is called the *module character of U_k*. The motivation for this name is as follows: for each intermediate field $L = \mathrm{GF}(q^l)$ of F_k over F, U_k carries the structure as an $L[x]$-module with respect to $\sigma_L = \sigma_F^l$ (see (1.2)), and conversely, if M is a subfield of E such that U_k is an $M[x]$-

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

module with respect to $\sigma_M = \sigma_F^{[M:F]}$, then, from the definition of F_k, M is a subfield of F_k, whence $[M : F]$ divides $\kappa(k)$.

Now, in analogy to the normal basis theorem, it holds that, for every intermediate field L of F_k over F, U_k is free on one generator as an $L[x]$-module (with respect to σ_L). Moreover, if $l = [L : F] = l'\beta$, β a power of p and l' prime to p, then the minimal polynomial of U_k as $L[x]$-module is equal to

$$\Phi_{k/l'}^{\pi/\beta}. \tag{4.3}$$

By [7, Theorem 18.8], similar to the strengthening of the normal theorem of Blessenohl and Johnsen [2], it even holds that U_k is *completely cyclic* in the following sense.

PROPOSITION 4.1. *Let E, F and k, π be as above. Then there exists an element $v \in U_k$ such that v simultaneously generates U_k as an $L[x]$-module for all intermediate fields L of $F_k = \mathrm{GF}(q^{\kappa(k)})$ over F. Such an element is called a* complete generator for U_k over F. *Moreover, the complete generators v of U_k are characterized by the following condition:*

$$\mathrm{ord}_{q^{d\delta}} v = \Phi_{k/d}(x^{\pi/\delta}) \tag{4.4}$$

for all d dividing $\frac{k}{\nu(k)}$ and all δ dividing π.

We will now give a characterization of the completely normal elements for a class of extensions which comprises the class of regular extensions. In fact, Theorem 4.2 includes a characterization of regularity for the case where n is not divisible by the characteristic p. A proof of Theorem 4.2 is given in [7, Section 19].

Observe first that the canonical decomposition

$$x^n - 1 = \prod_{k|m} \Phi_k^{\pi} \tag{4.5}$$

(where k runs over all positive divisors of m) corresponds to a decomposition of E into a direct sum of cyclotomic modules, i.e.,

$$E = \bigoplus_{k|m} U_k = \bigoplus_{k|m} U_{F,\Phi_k^{\pi}}. \tag{4.6}$$

For $w \in E$, let $\sum_{k|m} w_k$ be the decomposition of w with respect to the decomposition (4.6) of E.

THEOREM 4.2. *Let E be the field extension of degree $m\pi$ over $F = \mathrm{GF}(q)$, where m is not divisible by the characteristic p of F and where π is a power of p. If $w = \sum_{k|m} w_k \in E$ is completely normal over F, then for every divisor k of m, w_k is a complete generator for the cyclotomic module $U_{F,\Phi_k^{\pi}}$. Furthermore, the following statements are equivalent.*

1. *(q, m) is regular.*
2. *If $\{v_k : k|m\}$ is any collection of elements in E such that for every divisor k of m, v_k is a complete generator for the cyclotomic module $U_{F,\Phi_k^{\pi}}$, then $\sum_{k|m} v_k$ is completely normal in E over F.*

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

We summarize that, in a regular extension, the set of completely normal elements is precisely the sum of the sets of complete generators over all cyclotomic submodules.

Extending the notion of regularity, we call a cyclotomic module $U_k = U_{F,\Phi_k^\pi}$ *regular over* $F = \mathrm{GF}(q)$, if $(q, k\pi)$ is regular. Moreover, if U_k is regular, then it is called *exceptional* if $(q, k\pi)$ is exceptional.

We next give a characterization of the completely normal elements for regular but not exceptional extensions, and this characterization will be essential for our considerations in Section 5. For the proof of Theorem 4.3 we refer to [7, Section 20].

Remember first from (3.1) that for an integer k which is prime to q, the multiplicative order of q modulo k is of the form $\mathrm{ord}_{\nu(k)}(q) \cdot \prod_{r|k} r^{\alpha(r)}$, where the product runs over all prime divisors of k. We define the parameter $\tau(k)$ by

$$\tau(k) = \tau(q, k) := \prod_{r|k} r^{\lfloor \frac{\alpha(r)}{2} \rfloor}, \tag{4.7}$$

where, for a rational number ρ, $\lfloor \rho \rfloor$ denotes the integer part of ρ. It holds that $\tau(k)$ is a divisor of $k/\nu(k)$ (see [7, Lemma 20.5]), whence $U_k = U_{F,\Phi_k^\pi}$ carries the structure as an $L_k[x]$-module, where, throughout,

$$L_k := \mathrm{GF}(q^{\tau(k)}). \tag{4.8}$$

The minimal polynomial of U_k as $L_k[x]$-module is equal to Ψ_k^π, where

$$\Psi_k := \Phi_{k/\tau(k)}. \tag{4.9}$$

THEOREM 4.3. *Let U_{F,Φ_k^π} be a regular cyclotomic module over $F = \mathrm{GF}(q)$. Assume that $q - 1$ is divisible by 4 if q is odd and k is even. Then v is a complete generator of U_{F,Φ_k^π} if and only if the $q^{\tau(k)}$-order of v is equal to $\Psi_k^\pi = \Phi_{k/\tau(k)}^\pi$.*

If $(q, k\pi)$ is exceptional, then the set of complete generators of U_k over $\mathrm{GF}(q)$ does not allow a characterization as in the assertion of Theorem 4.3. For more details we refer to [7, Theorem 20].

5. Character sums and characteristic functions. In the present section, we use the theory of character and Gauss sums in order to obtain a sufficient number theoretical condition for the existence of a primitive completely normal element for an extension satisfying the assumption of Theorem 1.4. Throughout, we use the same notation as in Section 4.

Concerning the primitivity, for $w \in E$ let

$$M_{q,n}(w) := \frac{\varphi(q^n - 1)}{q^n - 1} \sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{(\eta,d)} \eta(w), \tag{5.1}$$

where, for the ring of integers, φ denotes the Euler totient function and μ the Möbius function. Furthermore, the second sum runs over all multiplicative characters of the field E having multiplicative order exactly d. It is well known (see e.g.

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

[**3**], [**5**] or [**12**]) that, with the convention $M_{q,n}(0) = 0$, $M_{q,n}$ is the characteristic function of the set of all w in E which are primitive, i.e., $M_{q,n}(w) = 1$ if w is primitive, and $M_{q,n}(w) = 0$, otherwise.

Assume next that k is a divisor of m. Furthermore, let l be a divisor of $k/\nu(k)$, whence l divides the module character $\kappa(k) = k\pi/\nu(k)$ of $U_k = U_{\Phi_k^\pi}$ (see (4.2)), and therefore $L = \mathrm{GF}(q^l)$ is an intermediate field of F_k over F. For $w \in E$ let

$$A_{q,l,k}(w) := \frac{\phi_{q^l}(\Phi_{k/l})}{q^{l\varphi(k/l)}} \sum_{g|_l \Phi_{k/l}} \frac{\mu_{q^l}(g)}{\phi_{q^l}(g)} \sum_{(\chi,g)_l} \chi(w), \tag{5.2}$$

where ϕ_{q^l} and μ_{q^l} denote the Euler function and the Möbius function, respectively, for the ring $L[x]$. Furthermore, $|_l$ indicates that the first sum runs over all monic L-divisors of $\Phi_{k/l}$, whereas $(\chi, g)_l$ indicates that the second sum runs over all additive characters of E having *L-order* (or *q^l-order*) exactly g. At this point we have to remark that the notion of L-order is also defined for the group $\hat{E}$ of additive characters of E, since $\hat{E}$ carries the structure as an $L[x]$-module by letting

$$(g \circ_L \chi)(w) := \chi(g \circ_L w), \quad \chi \in \hat{E},\ g \in L[x],\ w \in E, \tag{5.3}$$

where $\circ_L$ is as in (1.2) (see also [**12**], [**4**] or [**8**]). The L-order of $\chi \in \hat{E}$ is defined as the monic polynomial $f \in L[x]$ of least degree such that $f \circ_L \chi = \chi_0$, where χ_0 is the trivial additive character. As $L[x]$-modules, $\hat{E}$ and $(E, +)$ are isomorphic, whence every $L[x]$-submodule of $\hat{E}$ is free on one generator; in particular, as an $L[x]$-module, $\hat{E}$ is annihilated by $x^{n/l} - 1$. Furthermore, for each monic L-divisor g of $x^{n/l} - 1$ there are exactly $\phi_{q^l}(g) \geq 1$ additive characters whose L-order is equal to g (see e.g. [**12**]). By [**4**, Section 3] (here applied to the field extension E over L) it holds that $A_{q,l,k}$ is the characteristic function of the set of all w in E whose L-order is divisible by $\Phi_{k/l}^\pi$.

We assume now that E is a regular extension over F. For a divisor k of m, let $\tau(k) = \tau(q, k)$ be as in (4.7), L_k as in (4.8) and Ψ_k as in (4.9). For $w \in E$, let

$$\hat{A}_{q,n}(w) := \prod_{k|m} A_{q,\tau(k),k}(w). \tag{5.4}$$

Then the following essentially is a consequence of Theorem 4.3.

PROPOSITION 5.1. *Let E be the field extension of degree n over $F = \mathrm{GF}(q)$, and let $n = m\pi$ where m is not divisible by the characteristic p of F and π is a power of p. Assume that E is a regular extension over F. Assume further that $q - 1$ is divisible by 4 if q is odd and n is even. Then $\hat{A}_{q,n}$ is the characteristic function of the set of elements in E which are completely normal over F, i.e., $\hat{A}_{q,n}(w) = 1$ if w is completely normal over F and $\hat{A}_{q,n}(w) = 0$ otherwise.*

Proof. Assume first that w is completely normal in E over F. If k is a divisor of m, then $\tau(k)$ divides m, whence w is normal in E over L_k, and therefore the L_k-order of w is equal to $x^{n/\tau(k)} - 1$ which is divisible by Ψ_k^π. Consequently, $A_{q,\tau(k),k}(w) = 1$. Since this holds for all divisors k of m, we have that $\hat{A}_{q,n}(w) = 1$.

Assume conversely that $\hat{A}_{q,n}(w) = 1$ for some $w \in E$, i.e., $A_{q,\tau(k),k}(w) = 1$ for all divisors k of m. We fix a divisor e of m and let $\sum_{d|m/\tau(e)} \hat{w}_d$ be the decomposition of w with respect to the decomposition of E given by $\prod_{d|m/\tau(e)} \Phi_d^\pi$, i.e., as an $L_e[x]$-mod-

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

ule. Then $A_{q,\tau(e),e}(w) = 1$ if and only if $\Psi_e^\pi = \Phi_{e/\tau(e)}^\pi$ divides the $q^{\tau(e)}$-order of w, i.e., the L_e-order of w, and this is true if and only if $\hat{w}_{e/\tau(e)}$ has $q^{\tau(e)}$-order Ψ_e^π (this is an application of [7, Theorem 8.6]). Since

$$[L_e : F] = \tau(e) \text{ and } \Phi_e^\pi = \Psi_e^\pi(x^{\tau(e)}), \tag{5.5}$$

it furthermore holds that

$$U_{L_e,\Psi_e^\pi} = U_{F,\Phi_e^\pi} \tag{5.6}$$

(see also [7, Proposition 14.2]) and therefore $\hat{w}_{e/\tau(e)} = w_e$. Thus, $A_{q,\tau(e),e}(w) = 1$ if and only if w_e has L_e-order equal to Ψ_e^π. Since this holds for all divisors e of m, Theorem 4.3 implies that w is completely normal in E over F, and everything is proved. □

A straightforward application of (5.1) and Proposition 5.1 now gives a characterization of primitive completely normal elements for extensions as in Theorem 1.4.

COROLLARY 5.2. *Let E and F be as in Theorem 1.4. Then $w \in E$ is primitive and completely normal over F if and only if $M_{q,n}(w) \cdot \hat{A}_{q,n}(w) = 1$. Moreover, the number of elements of E which are primitive and completely normal over F is precisely equal to $\sum_{w\in E} M_{q,n}(w)\hat{A}_{q,n}(w)$.*

We now turn to the main result of this section, i.e., the announced sufficient number theoretical criterion. Throughout, let $\omega(q, n)$ denote the number of different prime divisors of $q^n - 1$. Moreover, for a divisor k of m let $\Omega_q(k)$ be the number of different monic divisors of Ψ_k which are irreducible over L_k, i.e.,

$$\Omega_q(k) := \frac{\varphi(\frac{k}{\tau(k)})}{\operatorname{ord}_{\frac{k}{\tau(k)}}(q^{\tau(k)})}. \tag{5.7}$$

Finally, let

$$\hat{\Omega}_q(n) := \sum_{k|m} \Omega_q(k). \tag{5.8}$$

THEOREM 5.3. *Let E be the field extension of degree $m\pi$ over $F = \mathrm{GF}(q)$, where m is not divisible by the characteristic p of F and where π is a power of p. Assume that E is a regular extension over F. Assume further that $q - 1$ is divisible by 4 if q is odd and n is even. If*

$$q^{\frac{n}{2}} > (2^{\omega(q,n)} - 1) \cdot (2^{\hat{\Omega}_q(n)} - 1), \tag{5.9}$$

then there exists an element $w \in E$ which is primitive and completely normal over F.

Proof. Let $X = \sum_{w\in E} M_{q,n}(w)\hat{A}_{q,n}(w)$ denote the number of elements $w \in E$ which are primitive and completely normal over F (see Corollary 5.2). We define

$$\theta := \frac{\varphi(q^n - 1)}{q^n - 1} \quad \text{and} \quad \hat{\Theta} := \prod_{k|m} \frac{\phi_{q^{\tau(k)}}(\Psi_k)}{q^{\varphi(k)}}. \tag{5.10}$$

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

Since $\tau(k)$ divides $k/\nu(k)$, we have

$$\varphi(k) = \tau(k) \cdot \varphi\left(\frac{k}{\tau(k)}\right),$$

and therefore the factor of $\hat{\Theta}$ indexed with k coincides with the first factor of $A_{q,\tau(k),k}$ (see (5.2)). Consequently, combining (5.1), (5.2), (5.4) and Corollary 5.2, we have

$$\frac{X}{\theta\hat{\Theta}} = \sum_{d|q^n-1} \sum_{g|\Psi} \frac{\mu(d)}{\varphi(d)} \prod_{k|m} \left(\frac{\mu_{q^{\tau(k)}}(g_k)}{\phi_{q^{\tau(k)}}(g_k)}\right) \sum_{(\eta,d)} \sum_{(\chi,g)} \Gamma(\eta, \chi), \tag{5.11}$$

where $g|\Psi$ indicates that the sum runs over all mappings g from the set D_m of positive divisors k of m to $E[x]$ such that $g(k) = g_k$ is a monic divisor of Ψ_k with coefficients in L_k. Moreover, for a given g, (χ, g) denotes the set of pairs of mappings from D_m to $\hat{E}$ and $E[x]$, respectively such that $\chi(k) = \chi_k$ has L_k-order g_k. Finally, $\Gamma(\eta, \chi)$ denotes the *Gauss sum*

$$\Gamma(\eta, \chi) = \sum_{w \in E} \eta(w)\left(\prod_{k|m} \chi_k\right)(w). \tag{5.12}$$

(As usual, we have written $\hat{E}$ multiplicatively.)

For a divisor k of m, let

$$C_{L_k, \Psi_k^\pi} = \{\alpha \in \hat{E} \mid \Psi_k^\pi \circ_{L_k} \alpha = 0\} \tag{5.13}$$

be the set of all additive characters having L_k-order dividing Ψ_k^π. Then C_{L_k,Ψ_k^π} is an $L_k[x]$-submodule of $\hat{E}$. Moreover, this set coincides with the $F[x]$-submodule C_{F,Φ_k^π} of $\hat{E}$ (see also (5.5) and (5.6)). Furthermore, analogously to (4.6), we have

$$\hat{E} = \bigoplus_{k|m} C_{L_k, \Psi_k^\pi} = \bigoplus_{k|m} C_{F, \Phi_k^\pi}, \tag{5.14}$$

where $\oplus$ here denotes a direct product of $F[x]$-submodules. In particular, the additive character $\prod_{k|m} \chi_k$ in the argument of the Gauss sum (5.12) is equal to the trivial additive character if and only if each component χ_k is trivial. (Observe that, because of (5.14), an additive character χ can be identified with a mapping from D_m to $\hat{E}$ by letting $\chi(k) = \chi_k$ be the C_{F,Φ_k^π}-component of χ.)

The further analysis of equation (5.11) is similar to that in [**11**], [**4**] or [**8**]: if η and χ are both trivial characters, then $\Gamma(\eta, \chi) = q^n$; if either η or χ is trivial, then $\Gamma(\eta, \chi) = 0$; if both, η and χ are nontrivial, then the absolute value of $\Gamma(\eta, \chi)$ is equal to $q^{n/2}$. A proof of the latter facts may be found in [**13**]. Now, substracting the q^n-term on both sides of (5.11) and taking absolute values we obtain

$$\left|\frac{X}{\theta\hat{\Theta}} - q^n\right| \leq q^{n/2} \cdot Y \cdot Z, \tag{5.15}$$

where, recalling properties of the Möbius functions, Y denotes the number of nontrivial multiplicative characters η occuring in (5.11) having square-free multiplicative

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

order, and where Z denotes the number of nontrivial additive characters χ such that χ_k has square-free L_k-order for each divisor k of m. A simple counting shows

$$Y = 2^{\omega(q,n)} - 1$$

and, by (5.7) and (5.8),

$$Z = \prod_{k|m} 2^{\Omega_q(k)} - 1 = 2^{\hat{\Omega}_q(n)} - 1.$$

Consequently, if $X = 0$, then

$$q^{\frac{n}{2}} \leq (2^{\omega(q,n)} - 1)(2^{\hat{\Omega}_q(n)} - 1),$$

and everything is proved. □

6. Primitivity and complete normality for regular extensions. In the present section we shall complete the proof of Theorem 1.4 by further investigating the sufficient criterion in Theorem 5.3. Throughout, we assume that $E = \mathrm{GF}(q^n)$ and $F = \mathrm{GF}(q)$ satisfy the assumptions of Theorem 1.4. We use the same terminology as in the foregoing sections, in particular, $n = m\pi$, where m is not divisible by the characteristic p of F and π is a power of p.

We first derive upper bounds for the parameters $\omega(q, n)$ and $\hat{\Omega}_q(n)$.

Assume that $l > 1$ is an integer and Λ is a set of primes $s \leq l$ such that each prime divisor of $q^n - 1$ which is less than l is contained in Λ. By [**12**, Lemma 2.6],

$$\omega(q, n) < \frac{n \log q - \log L(\Lambda)}{\log l} + |\Lambda|, \tag{6.1}$$

where

$$L(\Lambda) := \prod_{s \in \Lambda} s \tag{6.2}$$

and $|\Lambda|$ denotes the cardinality of Λ.

To obtain an upper bound for $\hat{\Omega}_q(n)$, recall from (5.7) and (5.8) that

$$\hat{\Omega}_q(n) = \sum_{k|m} \Omega_q(k) = \sum_{k|m} \frac{\varphi(\frac{k}{\tau(k)})}{\mathrm{ord}_{\frac{k}{\tau(k)}}(q^{\tau(k)})}.$$

Since (q, k) is regular, i.e., $\mathrm{ord}_{v(k)}(q)$ and k are relatively prime, Lemma 20.5 in [**7**] (see also (3.3)) gives

$$\mathrm{ord}_{\frac{k}{\tau(k)}}(q^{\tau(k)}) = \frac{\mathrm{ord}_k(q)}{\tau(k)^2}. \tag{6.3}$$

Recalling that $\varphi(k/\tau(k)) = \varphi(k)/\tau(k)$ (see also (5.10)), we obtain

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

$$\Omega_q(k) = \tau(k) \cdot \frac{\varphi(k)}{\mathrm{ord}_k(q)} = \frac{\varphi(k)}{\tau(k) \cdot \mathrm{ord}_{\frac{k}{\tau(k)}}(q^{\tau(k)})}, \tag{6.4}$$

and therefore

$$\hat{\Omega}_q(n) \leq \sum_{k|m} \frac{\varphi(k)}{\tau(k)}. \tag{6.5}$$

Taking $\tau(k) = 1$ for all k, one derives the trivial upper bound $\hat{\Omega}_q(n) \leq m$ from (6.5). In fact, if $\hat{\Omega}_q(n) = m$ then (q, n) is completely basic (this is a consequence of Proposition 3.3).

From now on, we assume that (q, n) is regular but not completely basic. Using Lemma 3.4, we then derive a bound for $\hat{\Omega}_q(n)$ which is much better than the trivial one. By Proposition 3.3 and Lemma 3.4 there exists a prime divisor r of m such that r^2 divides $\mathrm{ord}_{m_r}(q)$ where m_r is the maximal power of r dividing m; moreover, r^3 divides m. Since the τ-mapping is multiplicative (see (3.2), (4.7) and (4.8)), we obtain that $\tau(em_r)$ is divisible by r for each divisor e of $l := m/m_r$. This leads to the upper bound (6.6) for $\hat{\Omega}_q(n)$.First, using (6.5),

$$\sum_{k|\frac{m}{m_r}} \Omega_q(km_r) \leq \sum_{k|\frac{m}{m_r}} \frac{\varphi(km_r)}{r} = \frac{m}{m_r} \cdot \frac{\varphi(m_r)}{r} = \frac{m(r-1)}{r^2},$$

and therefore

$$\hat{\Omega}_q(n) = \sum_{k|\frac{m}{r}} \Omega_q(k) + \sum_{k|\frac{m}{m_r}} \Omega_q(km_r) \leq \frac{m}{r} + \frac{m(r-1)}{r^2} = \frac{2r-1}{r^2} \cdot m. \tag{6.6}$$

Summarizing, the combination of (6.1) and (6.6) gives the following sufficient criterion for the existence of a primitive completely normal element in E over F. We leave the details to the reader.

THEOREM 6.1. *Let E be the field extension of degree n over $F = \mathrm{GF}(q)$. Let $n = m\pi$, where m is not divisible by the characteristic p of F and where π is a power of p. Assume that E is regular over F but not completely basic. Assume further that $q - 1$ is divisible by 4 if q is odd and n is even. Next, let $l > 1$ be an integer, let Λ be a set of primes $s < l$ such that each prime divisor of $q^n - 1$ which is less than l is contained in Λ, and let $L(\Lambda)$ be as in (6.2). Finally, let r be a prime divisor of m such that $\mathrm{ord}_{m/r}(q)$ is divisible by r, and let $\rho \leq r$ and δ be a divisor of π. If*

$$\left(\frac{n}{\log 4} - \frac{n}{\log l}\right) \cdot \log q \geq \frac{2\rho - 1}{\rho^2} \cdot \delta m + |\Lambda| - \frac{\log L(\Lambda)}{\log l}, \tag{6.7}$$

then there exists a primitive element in E which additionally is completely normal over F.

We are now able to finish the proof of Theorem 1.4. Assume that (q, n) satisfies the assumptions of Theorem 1.4 and by contradiction that no primitive element in $E = \mathrm{GF}(q^n)$ is completely normal over $F = \mathrm{GF}(q)$.

By Lemma 3.4, m is divisible by a cube of a prime r. Moreover, if m is not divisible by the cube of an odd prime, then 16 divides m. In particular, $n \geq m \geq 16$.

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

We take $l = 68$, $\delta m = n$, $\rho = 2$ and let Λ_l be the set of all primes $s < l$. Then an application of Theorem 6.1 shows that

$$\log q < \frac{3}{4a} + \frac{1}{na} \cdot \left(|\Lambda_l| - \frac{\log L(\Lambda_l)}{\log l} \right), \tag{6.8}$$

where $a = 1/\log 4 - 1/\log l$. This implies $q \leq 9$.

Moreover, if q is even, then $n \geq m \geq 27$; if $q = 7$ then n is odd and $m \geq 27$. Thus, using the factor $5/9$ instead of $3/4$ in (6.8) gives a contradiction if $q = 8$ or $q = 7$. If $q = 3$ then n is odd and $m \geq 125$. We can therefore use the factor $9/25$ instead of $3/4$ in (6.8) and again obtain a contradiction. This leaves the cases $q = 9$, $q = 5$, $q = 4$ and $q = 2$.

If $q = 9$, then (using the same parameters $l, \delta, \rho, \Lambda_l$ as above) gives $n \leq 17$ by Theorem 6.1. This leaves the only possibility $n = 16$. But $(9, 16)$ is completely basic, a contradiction.

If $q = 5$ then (with the same parameters as above) we obtain $n \leq 183$ by Theorem 6.1. Observing that all pairs $(5, 8 \cdot 5^a)$ are completely basic, it remains to consider the cases where m is divisible by 16 or by the cube of an odd prime. This leaves the cases where n is equal to one of the following numbers

$$16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 27, 54, 81, 108, 135, 162.$$

We can exclude $n = 48, 96, 112, 144, 54, 108, 162$ since the corresponding pairs are not regular. If $n \in \{27, 81, 135\}$ we apply Theorem 6.1 with l and Λ_l as before, but with $\rho = 3$, and obtain the contradiction $n \leq 23$. For the rest, i.e., $n = 16, 32, 64, 80, 128, 160, 176$, we apply Theorem 6.1 with $\rho = 2$ and l as above, but this time, we can use for Λ the set of all primes $s < 68$ different from 5 and where $\mathrm{ord}_s(q)$ is a power of 2 (for $n = 16, 32, 64, 128$), or 5 times a power of 2 (for $n = 80, 160$), or 11 times a power of 2 (for $n = 176$), respectively. In all cases we obtain a contradiction.

If $q = 4$, we apply Theorem 6.1 with $l = 68$ and Λ being the set of odd primes less than 68. Moreover, we may choose $\rho = 3$. This gives $n \leq 46$, whence it remains to consider the case $n = 27$. But with Λ being the set of all primes $s < 68$, different from 2, for which $\mathrm{ord}_s(4)$ is a power of 3, Theorem 6.1 gives a contradiction.

Finally, let $q = 2$. Then m is odd and thus, for every divisor k of m, $\mathrm{ord}_{v(k)}(q)$ is at least equal to 2. Since $\mathrm{ord}_{v(k)}(q)$ divides $\mathrm{ord}_k(q)/\tau(k)^2$ (see (6.3), (4.7) and (3.1)), (6.4) can be improved to $\Omega_q(k) \leq \phi(k)/(2\tau(k))$ and therefore we can improve (6.6) to

$$\hat{\Omega}_2(n) \leq \frac{1}{2} \cdot \frac{2r-1}{r^2} \cdot m,$$

where $r \geq 3$. The smallest case $r = 3$ gives $\hat{\Omega}_2(n) \leq \frac{5}{18} m$. With this data and with $l = 68$ and Λ_l as above, an application of Theorem 6.1 shows $n \leq 93$, leaving the cases $n = 27, 54, 81$. However, using once more Theorem 6.1 with Λ being the set of all primes $s < 68$, different from 2, for which $\mathrm{ord}_s(2)$ divides 162 gives a contradiction for all the remaining values of n.

This completes the proof of Theorem 1.4. □

https://doi.org/10.1017/S0017089501030026 Published online by Cambridge University Press

7. Concluding remarks. We have proved the existence of primitive completely normal elements for the considerably large class of regular extensions E over a finite field F which are not exceptional. Concerning Problem 1.1 in full generality, there occur two main difficulties.

First, if (q, m) is not regular and m is prime to q, then with $n = m\pi$, the set of completely normal elements is a proper subset of the direct sum of the sets of complete generators over the cyclotomic submodules of E. Thus, completely normal elements cannot be characterized by means of the decomposition (4.6), i.e., Theorem 4.2 is not valid. Nevertheless, as shown in Section 19 of [7], there still exist nontrivial decompositions of E allowing a characterization of completely normal elements in terms of the components of the decompositions (those decompositions are called *agreeable* in [7]). In the theory developed in [7], the canonical decomposition (4.5) is the *finest* possible agreeable decomposition.

Secondly, if (q, m) is exceptional or not regular and if Δ is an agreeable decomposition of E, then there are components of Δ whose set of complete generators cannot be characterized by a certain single module structure as in Theorem 4.3.

While there are satisfactory results on simultaneous module structures and in particular on the nature of completely normal elements (see [7], [9]), the effective handling of these structures in terms of character sums seems to be very difficult but essential for solving Problem 1.1 in greater generality.

REFERENCES

1. D. Blessenohl and K. Johnsen, Eine Verschärfung des Satzes von der Normalbasis, *J. Algebra* **103** (1986), 141–159.

2. D. Blessenohl and K. Johnsen, Stabile Teilkörper Galoisscher Erweiterungen und ein Problem von C. Faith, *Archiv Math.* **56** (1991), 245–253.

3. L. Carlitz, Primitive roots in a finite field, *Trans. Amer. Math. Soc.* **73** (1952), 373–382.

4. S. D. Cohen and D. Hachenberger, Primitive normal bases with prescribed trace, *Applicable Algebra in Engineering, Communication and Computing* **9** (1999), 383–403.

5. H. Davenport, Bases for finite fields, *J. London Math. Soc.* **43** (1968), 21–49.

6. C. C. Faith, Extensions of normal bases and completely basic fields, *Trans. Amer. Math. Soc.* **85** (1957), 406–427.

7. D. Hachenberger, *Finite Fields: Normal Bases and Completely Free Elements* (Kluwer Academic Publishers, Boston, 1997).

8. D. Hachenberger, Primitive normal bases for towers of field extensions, *Finite Fields and their Applications* **5** (1999), 378–385.

9. D. Hachenberger, A decomposition theory for cyclotomic modules under the complete point of view, *J. Algebra* **237** (2001), 470–486.

10. K. Hensel, Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, *J. Reine Angew. Mathematik* **103** (1888), 230–237.

11. N. Koblitz, *A Course in Number Theory and Cryptography*, second edition (Springer, Berlin, 1994).

12. H. W. Lenstra, Jr. and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comp.* **48** (1987), 217–231.

13. R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley, Reading, Massachusetts, 1983).

14. I. H. Morgan and G. L. Mullen, Completely normal primitive basis generators of finite fields, *Utilitas Math.* **49** (1996), 21–43.

15. G. L. Mullen and I. Shparlinski, Open problems and conjectures in finite fields, in: Proc. Third International Conference on Finite Fields and Applications, Glasgow, 1995,

(Eds.: S.D. Cohen and H. Niederreiter), L.M.S. Lecture Notes Series **233**, Cambridge University Press, Cambridge, (1996), 243–268.

16. E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, *J. Reine Angew. Mathematik* **167** (1932), 147–152.