Completely free elements

Dirk Hachenberger

Angaben zur Veröffentlichung / Publication details:

Hachenberger, Dirk. 1996. "Completely free elements." In *Finite fields and applications: Proceedings of the third international conference, Glasgow, July 1995*, edited by Stephen D. Cohen and Harald Niederreiter, 97–107. Cambridge: Cambridge University Press.

Completely Free Elements

Dirk Hachenberger

Abstract. This paper is a working out of the same-titled talk given by the author at the Third International Conference on Finite Fields and Their Applications in Glasgow, 1995. We give a survey on recent results on the characterization, the structure, the enumeration, and the construction of completely free elements and normal bases in finite dimensional extensions over finite fields.

1. A Strengthening of the Normal Basis Theorem. If E is a finite dimensional Galois extension over a field F with Galois group G, then the Normal Basis Theorem states that the additive group $(E,+)$ of E is a cyclic module over the group algebra FG, i.e., there exists an element w in E such that the set $\{g(w) \mid g \in G\}$ of *G-conjugates* of w is an F-basis of E. Such a basis is called a *normal basis in E over F*. Every generator w of E as FG-module is called a *normal basis generator in E over F*. For the sake of simplicity such an element is also called *free in E over F*.

If H is a subgroup of G, and $\mathrm{Fix}(H)$ is the intermediate field of E over F belonging to H via the Galois correspondence, i.e., the subfield of E which is fixed elementwise by H, then $(E,+)$ likewise carries the structure of a $\mathrm{Fix}(H)H$-module. Again, this module is cyclic; its generators are exactly those elements whose H-conjugates build a $\mathrm{Fix}(H)$-basis of E, i.e., the normal basis generators or free elements in E over $\mathrm{Fix}(H)$.

Considering simultaneously *all* module structures of $(E,+)$ arising from the intermediate fields of E over F together with the corresponding Galois groups, it is natural to ask whether a stronger version of the Normal Basis Theorem holds:

Do there exist elements in E which *simultaneously* are free over *every* intermediate field of E over F?

Such elements are called *completely free in E over F*.

This problem was first considered by C. Faith [4] in 1957. He proved existence in the case where the ground field F has infinite cardinality by generalizing Artin's proof of the Normal Basis Theorem [1]. Indeed, since Artin's argument also applies to finite fields provided the cardinality of the ground field is large enough, one can show that for every integer $m \geq 1$ there

exist at most finitely many prime powers $q > 1$ such that the Galois field $\mathrm{GF}(q^m)$ does not contain an element which is completely free over $\mathrm{GF}(q)$. The general problem, however, is not solved by this argument.

It was only in 1986 that D. Blessenohl and K. Johnsen [3] affirmatively settled the existence in the case of arbitrary finite fields. Their proof essentially relies on the fact that the Galois groups occuring are cyclic and gives more insight into the structure and nature of completely free elements. Altogether, the following holds:

Theorem 1.1 *Let E be a finite dimensional Galois extension over F, and let $\mathcal{K}$ be any nonempty set of intermediate fields of E over F. Then there exists an element in E which simultaneously is free over K for every $K \in \mathcal{K}$.*

A look at the Section 'Open Problems and Conjectures' of the proceeding volumes of the latest International Conferences on Finite Fields and Their Applications shows that completely free elements have attained much interest, lately. Here, it is our aim to give a survey on recent results obtained by the author on the characterization, the structure, the enumeration, and the construction of such elements, and, on normal bases in general in finite fields. It is our aim to give an idea of the nature of completely free elements. For details, proofs, and examples which illustrate these results, we refer to the three papers [5], [6] and [7], and mainly to the monograph [8], which is an extensive treatment of normal bases, completely free elements, and the structure of algebraic extensions over finite fields.

As standard references for the theory of finite fields, their arithmetic, and their applications, we refer to the books of R. Lidl and H. Niederreiter [11] and D. Jungnickel [10]. For the general algebraic background reference is made to N. Jacobson [9].

2. The Existence of Completely Free Elements.

Throughout, we assume that E and F are finite fields (although some of the results also hold under more general conditions). Basically, Blessenohl and Johnsen's proof of the existence of completely free elements in finite fields (see [3]) consists of two parts. First, similar as in the case of ordinary normal basis generators, the existence is easily reduced to extensions of prime power degree.

Reduction Theorem. *If u and v are completely free in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$ and $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$, respectively, and if n and m are relatively prime, then uv is completely free in $\mathrm{GF}(q^{mn})$ over $\mathrm{GF}(q)$.*

Thus, let r be a prime number, and assume that E is the r^n-dimensional extension over $F = \mathrm{GF}(q)$, where $n \geq 1$ is some integer. Then, two further

cases have to be considered, dependent on whether r is the characteristic of F or not. The following result, which is already due to Faith [4], deals with the case where r is the characteristic of F.

Theorem 2.1 *Consider $E = \mathrm{GF}(q^{r^n})$ over $F = \mathrm{GF}(q)$, where r is equal to the characteristic of F, and where $n \geq 1$ is an integer. Then the following statements are equivalent:*

(1) *The (E, F)-trace of $w \in E$ is nonzero.*

(2) *w is free in E over F.*

(3) *w is completely free in E over F.*

The case where r is different from the characteristic of F is the real difficult one. We postpone this part, since it is covered by results we are going to present in the next sections. The original, difficult to follow proof of Blessenohl and Johnsen essentially uses representation theory of abelian groups applied to cyclic Galois extensions. In [5], we have given a simpler proof of this difficult part. Our approach is mainly based on linear algebra and properties of cyclotomic polynomials which occur as annihilators of particular submodules of the extension field considered. This approach likewise leads to concreter, much more general results, and to the decomposition theory which we are going to outline in the next section. Already in extensions of prime power degree, we were able to determine the exact number of completely free elements (see [5]). Moreover, in [6] and [7] we have given explicit constructions of completely free elements in every prime power extension over every finite field, whence via the Reduction Theorem explicit constructions of completely free elements in any finite dimensional extension over any finite field are available. In particular this gives constructions of ordinary normal bases in arbitrary finite dimensional extensions over any finite field.

3. Decompositions of Completely Free Elements. If for example we consider the 1296-dimensional extension over GF(13), the Reduction Theorem and results from [5] give that there are at least 12^{96} completely free elements in that extension. Actually, the number of such elements in that extension is at least 12^{1296}. Consequently, the Reduction Theorem does not give a characterization. However, in this section we will see that completely free elements can be characterized by certain decompositions. We need some definitions and first recall well known results on ordinary normal basis generators. These go back to the fundamental work of O. Ore [13].

Let $E = \mathrm{GF}(q^m)$, $F = \mathrm{GF}(q)$, and let σ denote the *Frobenius automorphism in E over F*, i.e., the canonical generator of the Galois group G of

E over F mapping every w in E to its qth power. Since the Galois group is cyclic and σ in particular is an F-linear mapping on E, the FG-module structure of the additive group of E can be studied with tools from linear algebra: We consider E as a cyclic σ-invariant F-space.

With respect to this structure, the annihilator ideal of $(E,+)$ is generated by the polynomial x^m-1. The σ-invariant F-subspaces of E correspond bijectively to the monic divisors of x^m-1 with coefficients in F (the submodule corresponding to f is $U_f := \{v \in E | f(\sigma)(v) = 0\}$). Every submodule is cyclic. For $w \in E$, the *q-order of w* is defined to be the monic polynomial of least degree which annihilates w (it is denoted by $\mathrm{Ord}_q(w)$). The generators of U_f are exactly those elements in E whose q-order is equal to f. In particular, the elements in E which are free over F are exactly those whose q-order is equal to x^m-1.

Now, a *decomposition Δ of x^m-1 over F* is a set of monic divisors of x^m-1 with coefficients in F such that different members of Δ are relatively prime, and $x^m-1 = \prod_{\delta\in\Delta}\delta$.

The following well known theorem gives a characterization of free elements in E over F in terms of a decomposion of x^m-1 over F.

Theorem 3.1 *Consider the extension $E = \mathrm{GF}(q^m)$ over $F = \mathrm{GF}(q)$ and let Δ be a decomposition of x^m-1 over F. Then the following holds:*

(1) *$\bigoplus_{\delta\in\Delta} U_\delta$ is a decomposition of $(E,+)$ into σ-invariant F-spaces, i.e., every $w \in E$ can uniquely be written as $\sum_{\delta\in\Delta} w_\delta$ with $w_\delta \in U_\delta$ for all $\delta \in \Delta$.*

(2) *$\mathrm{Ord}_q(w) = \prod_{\delta\in\Delta}\mathrm{Ord}_q(w_\delta)$ for all $w \in E$.*

(3) *w is free in E over F if, and only if $\mathrm{Ord}_q(w_\delta) = \delta$ for all Δ-components w_δ of w.*

Consequently, if for a given decomposition Δ of x^m-1 a generator of each Δ-component is known, then we have a free element.

Now, in order to find completely free elements, in analogy to Theorem 3.1, we consider the problem whether there are decompositions Δ of x^m-1 over F satisfying the following property:

(*) *Every* completely free element can be characterized by the properties of its Δ-components, and, *every* completely free element can be constructed by working *independently* on the Δ-components.

Observe, however, that there is an essential difference considering completely free instead of free elements:

In the case of free elements, Theorem 3.1 is natural, since every Δ leads to a decomposition of $(E,+)$ which respects the *only* module structure considered. In contrast, the definition of completely free requires that $(E,+)$ has to

be simultaneously generated with respect to *all* its module structures arising from the intermediate fields of E over F. Hence, for all positive divisors d of m, we have to consider $(E,+)$ simultaneously as $\mathrm{GF}(q^d)$-vector space with respect to σ^d (we choose σ^d as generator of the corresponding Galois group). But, since no nontrivial subgroup of $(E,+)$ can simultaneously be invariant under all these module actions, the existence of a nontrivial decomposition satisfying (*) is a nontrivial problem.

On the other hand, the existence of a nontrivial decomposition satisfying (*) implies that in order to characterize completely free elements not all module structures actually have to be considered simultaneously. Thus, necessarily, the simultanity is "distributed over the components" of such a decomposition.

Throughout, we will make the latter ideas precise. The only restriction we make is that the degree m of the extension is relatively prime to the cardinality q of the ground field. This implies that the polynomial $x^m - 1$ is square-free over $\mathrm{GF}(q)$. Though technically more involved, the results can be extended to the general case.

In order to describe how to find a nontrivial decomposition satisfying (*), we introduce further definitions:

Let $k, t \geq 1$ be integers, and let Φ_k be the kth cyclotomic polynomial. A polynomial λ of the form $\lambda = \Phi_k(x^t)$ is called *suitable over* $\mathrm{GF}(q)$, provided k and t are relatively prime to q (in which case λ is square-free). Due to fundamental properties of cyclotomic polynomials, we may without loss of generality assume that k and t are relatively prime.

A decomposition Δ of $x^m - 1$ over $\mathrm{GF}(q)$ is called *suitable*, provided that δ is suitable over $\mathrm{GF}(q)$ for every δ in Δ.

A suitable decomposition of $x^m - 1$ over $\mathrm{GF}(q)$ is called *agreeable over* $\mathrm{GF}(q)$, if it satisfies (*).

These definitions are motivated by the fact that $x^m - 1 = \Phi_1(x^m)$ is a suitable polynomial, and that, trivially, $\{x^m - 1\}$ is an agreeable decomposition of $x^m - 1$ over $\mathrm{GF}(q)$. Now, the following theorem gives a necessary condition which states when an agreeable decomposition of $x^m - 1$ over $\mathrm{GF}(q)$ can be refined.

Theorem 3.2 *Let Δ be an agreeable decomposition of $x^m - 1$ over $\mathrm{GF}(q)$. Let $\lambda = \Phi_k(x^t)$ be an element of Δ (with k and t being relatively prime), and let r be a prime divisor of t. Assume that R is the largest power of r dividing t. Furthermore, let $\Sigma := \{\Phi_k(x^{\frac{t}{r}}), \Phi_{kR}(x^{\frac{t}{R}})\}$, and let $\Gamma := \Delta - \{\lambda\} \cup \Sigma$. Then the following holds:*

(1) *Γ is a suitable decomposition of $x^m - 1$ over $\mathrm{GF}(q)$.*

(2) *If the multiplicative order of q modulo the square-free part of kt is not divisible by R, then Γ is an agreeable decomposition of $x^m - 1$ over* GF(q).

We remark that Theorem 3.2 always is applicable to the trivial decomposition $\{\Phi_1(x^m)\}$ with r being the largest prime divisor of m, in which case we obtain the nontrivial agreeable decomposition $\{x^{\frac{m}{r}} - 1, \Phi_R(x^{\frac{m}{R}})\}$ (where R is the largest power of r dividing m). This shows that nontrivial agreeable decompositions of $x^m - 1$ always do exist!

As an example, consider the 42-dimensional extension over GF(5). Repeated application of Theorem 3.2 shows that $\{x - 1, x + 1, \Phi_3(x^2), \Phi_7(x^6)\}$ is an agreeable decomposition of $x^{42} - 1$ over GF(5). Moreover, Theorem 3.2 cannot be applied to any of its components.

It is an open problem whether the refinement condition (2) in Theorem 3.2 is necessary.

Once an agreeable decomposition has been found, it remains to characterize the components of completely free elements with respect to this decomposition. This is done in the following two theorems.

Theorem 3.3 *Let Δ be an agreeable decomposition of $x^m - 1$ over* GF(q), *where q and m are relatively prime. For $w \in E$ let $\sum_{\delta\in\Delta} w_\delta$ be the decomposition of w with respect to Δ. Then w is completely free over F if, and only if for all $\delta \in \Delta$, w_δ simultaneously generates U_δ with respect to all module structures arising from the intermediate fields of E over F which leave U_δ invariant.*

In order to make the characterizing condition in Theorem 3.3 more precise, properties of cyclotomic polynomials turn out to be very helpful. First, one can show the following:

Let $\lambda = \Phi_k(x^t)$ be a suitable divisor of $x^m - 1$ over GF(q), and let U_λ be the σ-invariant F-subspace of E corresponding to λ. Then, for a positive divisor d of m, U_λ is GF(q^d)-invariant if, and only if d divides $\frac{tk}{\mu(k)}$, where $\mu(k)$ denotes the square-free part of k. Therefore, the module structures arising from intermediate fields of E over F which leave U_λ invariant correspond bijectively to the poitive divisors of $\frac{tk}{\mu(k)}$. Furthermore, as σ^d-invariant GF(q^d)-space, U_λ is annihilated by the polynomial $\Phi_{\mu(k)}(x^{\frac{tk}{\mu(k)d}})$. Therefore, Theorem 3.3 can be formulated as follows:

Theorem 3.3' *Let Δ be an agreeable decomposition of $x^m - 1$ over* GF(q), *where q and m are relatively prime. For $w \in E$ let $\sum_{\delta\in\Delta} w_\delta$ be the decomposition of w with respect to Δ. Then w is completely free over F if, and only if the following holds for all $\delta \in \Delta$:*

If $\delta = \Phi_k(x^t)$, *then* $\mathrm{Ord}_{q^d}(w_\delta) = \Phi_{\mu(k)}(x^{\frac{tk}{\mu(k)d}})$ *for all positive divisors* d *of* $\frac{tk}{\mu(k)}$, *where* $\mu(k)$ *denotes the square-free part of* k.

We remark that in the case where Δ is the trivial agreeable decomposition $\{x^m - 1\}$, Theorem 3.3' results in the obvious fact that w is completely free over F if, and only if $\mathrm{Ord}_{q^d}(w) = x^{\frac{m}{d}} - 1$ for all nonnegative divisors d of m.

However, already if we look at the agreeable decomposition $\{x^{\frac{m}{r}} - 1, \Phi_R(x^{\frac{m}{R}})\}$, where r is the largest prime dividing m, and where R is the largest power of r dividing m, we can illustrate the effect which early in this Section we described as "distribution of simultanity over a decomposition": An application of Theorem 3.3' gives that it is sufficient to require the module structures arising from divisors of $\frac{m}{r}$; not all divisors of m have to be considered.

As a further example, look at the 42-dimensional extension over GF(5). The agreeable decomposition given subsequently to Theorem 3.2 shows that, instead of the 8 module structures arising from positive divisors of 42, it is sufficient to simultaneously require at most 4 module structures (for $\lambda = \Phi_7(x^6)$ we have to consider those corresponding to the positive divisors of 6).

It remains to show how components of a completely free element with respect to a given agreeable decomposition can actually be found. This problem is solved in general in [8]. Here, we restrict our attention to a particular class of extensions and just mention that the general case via a generalization of the Reduction Theorem can be reduced to particular *basic classes* of extensions. The class considered in the next section is such a basic one. There, fortunately, the problem can easily be solved.

4. Regular Extensions. In this section we characterize those pairs (q, m), for which q and m are relatively prime, and the *canonical decomposition* $\prod_{d|m} \Phi_d$ is agreeable over GF(q). By definition (see Section 3) the canonical decomposition is the finest suitable decomposition of $x^m - 1$ over GF(q). For simplicity those pairs (q, m) and the corresponding extensions are called *regular*.

The following result shows that regularity can be characterized by a simple number theoretical condition on q and m.

Theorem 4.1 *Consider* GF(q^m) *over* GF(q), *where* m *and* q *are relatively prime. Then the extension is regular if, and only if* m *and the multiplicative order of* q *modulo the square-free part of* m *are relatively prime.*

We remark that this number theoretical condition e.g. always holds in the case where m is a prime power. Trivially, further examples are the pairs (q, m) where $q - 1$ is divisible by the square-free part of m. However, there

are also other examples available, e.g., if all prime divisors of m belong to $\{5, 7, 13, 17, 19, 37\}$, and q is relatively prime to m, then the multiplicative order of q modulo the square-free part of m divides the least common multiple of $\{5-1, 7-1, 13-1, 17-1, 19-1, 37-1\}$ which is equal to 36. Thus, the multiplicative order of q modulo the square-free part of m is relatively prime to m.

In order to obtain a completely free element in a regular extension, by Theorem 3.3', for every positive divisor k of m we have to find an element w_k satisfying $\mathrm{Ord}_{q^d}(w_k) = \Phi_{\mu(k)}(x^{\frac{k}{\mu(k)d}}) = \Phi_{\frac{k}{d}}$ for all positive divisors d of $\frac{k}{\mu(k)}$, where $\mu(k)$ is the square-free part of k. Amazingly, the number theoretical condition which characterizes regularity also assures that up to some *exceptional pairs* (q, m) every such element can be characterized as the generator of U_{Φ_k} with respect to *one* particular module structure. (For an integer m, let m_2 be the largest power of 2 dividing m. Then (q, m) is called *exceptional*, if 8 divides m_2, if the multiplicative order of q modulo m_2 is equal to 2, and if q is not congruent to $1 + \frac{m_2}{2}$ modulo m_2.) Fortunately, the exceptional cases can also be handled.

Theorem 4.2 *Let m and q be relatively prime, let $\mathrm{GF}(q^m)$ be a regular extension over $\mathrm{GF}(q)$, and assume that (q, m) is not exceptional. For an element $w \in \mathrm{GF}(q^m)$ let $\sum_{k|m} w_k$ be the decomposition of w corresponding to the canonical decomposition of $x^m - 1$. Then the following holds:*

For every divisor k of m there exists a divisor $\tau(q, k)$ of $\frac{k}{\mu(k)}$ only depending on k and q, such that w is completely free in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$ if, and only if w_k generates U_{Φ_k} as $\sigma^{\tau(q,k)}$-invariant $\mathrm{GF}(q^{\tau(q,k)})$-vector space, i.e., if, and only if $\mathrm{Ord}_{q^{\tau(q,k)}}(w_k) = \Phi_{\mu(k)}(x^{\frac{k}{\mu(k)\tau(q,k)}}) = \Phi_{\frac{k}{\tau(q,k)}}$.

Altogether, we can summarize our results as follows: After having divided the whole problem of determining a completely free element into appropriate parts, in a large class of field extensions, the problem can algorithmically be solved by determining a generator of a cyclic vector space. This can e.g. be done by applying H. Lüneburg's algorithm which computes the rational normal form of an endomorphism (see [12]). In Section 5, we give explicit constructions of such elements.

We finally remark that, as a further consequence of Theorem 4.2, the exact number of completely free elements in regular extensions can be determined. In particular we have:

Theorem 4.3 *Let $\mathrm{GF}(q^m)$ be a regular extension over $\mathrm{GF}(q)$. Then the number of completely free elements in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$ is at least $(q-1)^m$.*

5. Explicit Constructions. Observing that $(q^d, \frac{m}{d})$ is regular, provided that (q, m) is regular, and due to the content of Theorem 4.2, we here consider the following basic problem (where again, the Q-order is defined with respect to the Frobenius automorphism over $\mathrm{GF}(Q)$):

Assume that (Q, K) is regular. Given the finite field $\mathrm{GF}(Q)$, find an element v in $\mathrm{GF}(Q^K)$ having Q-order Φ_K.

This problem is solved by the following two theorems. (The exceptional cases mentioned in Section 4 can similarly be handled.) First, a certain element whose Q-order has a particular form is given.

Theorem 5.1 *Let (Q, K) be a regular pair, let s be the multiplicative order of Q modulo the square-free part of K, and let $\rho = \rho(Q, K)$ be the largest divisor of $Q^s - 1$ whose prime divisors all consist of prime divisors of K.*

Furthermore, let η be a primitive ρKth root of unity.

Then $\mathrm{GF}(Q^{Ks})$ is obtained by adjoining η to $\mathrm{GF}(Q)$, and the Q-order of η is of the form $f(x^s)$, where f is a divisor of Φ_K which is irreducible over $\mathrm{GF}(Q)$.

Next, with the same notation as in Theorem 5.1, let Tr denote the trace function of $\mathrm{GF}(Q^{Ks})$ onto $\mathrm{GF}(Q^K)$. Using the fact that s and K are relatively prime, it can be shown that the Q-order of $\mathrm{Tr}(\eta)$ is an irreducible $\mathrm{GF}(Q)$-divisor of Φ_K. Hence, similar as in Theorem 3.1 for free elements, it remains now to find a set of elements in $\mathrm{GF}(Q^K)$ whose Q-orders correspond bijectively to the set of monic divisors of Φ_K which are irreducible over $\mathrm{GF}(Q)$. Then the sum of these elements constitutes an element having Q-order Φ_K. A construction of such a set is given in the following theorem.

Theorem 5.2 *Additionally to the assumptions of Theorem 5.1, let a be the greatest common divisor of ρ and K, let I be a set of representatives of units modulo a, and let J be a complete set of Q-orbit representatives of I (i.e., assume that j' is not congruent to jQ^l modulo a for each integer l and any different j and j' in J).*

Then $\{\mathrm{Ord}_Q(Tr(\eta^j)) | j \in J\}$ is equal to the set of monic divisors of Φ_K which are irreducible over $\mathrm{GF}(Q)$. Moreover, $Tr(\sum_{j\in J} \eta^j)$ generates U_{Φ_K} as Σ-invariant $\mathrm{GF}(Q)$-space, where Σ is the Frobenius automorphism over $\mathrm{GF}(Q)$.

6. Concluding Remarks. The decomposition theory and again properties of cyclotomic polynomials can be used to give iterative constructions of series of elements which are completely free in suitable extensions over the

ground field considered. One only has to guarantee that all decompositions are agreeable. For the case of regular extensions this is illustrated in the following theorem.

Theorem 6.1 *Let (q,m) be a regular pair, and let w be a completely free element in* $\mathrm{GF}(q^m)$ *over* $\mathrm{GF}(q)$. *Let $n > 1$ be an integer such that (q,mn) is regular. Let D be the set of positive divisors of mn which are not divisors of m. For every $d \in D$, let v_d be an element which simultaneously generates U_{Φ_d} with respect to all module structures arising from intermediate fields of* $\mathrm{GF}(q^{mn})$ *over* $\mathrm{GF}(q)$ *which leave U_{Φ_d} invariant.*

Then $w + \sum_{d\in D} v_d$ is completely free in $\mathrm{GF}(q^{mn})$ *over* $\mathrm{GF}(q)$.

Moreover, every element in $\mathrm{GF}(q^{mn})$ *which is completely free over* $\mathrm{GF}(q)$ *can be obtained in this manner.*

We finally remark that in the recent papers Blake, Gao and Mullin [2] and Scheerhorn [14], [15] there are given constructions of series of irreducible polynomials whose roots are completely free over the field considered. The extensions $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$ which are covered by these constructions are those, where m is a power of 2 (see [2]), or where m is odd and all prime divisors of m divide $q-1$ (see [2] and [14]), or where m is odd and all prime divisors of m divide $q+1$ (see [15]).

References

[1] E. ARTIN, "Galoissche Theorie." Harri Deutsch Verlag, Zürich, Frankfurt, 1973 (2nd Edition).

[2] I.F. BLAKE, X. GAO AND R.C. MULLIN, Specific Irreducible Polynomials with Linearly Independent Roots over Finite Fields. *Linear Algebra and its Applications*, submitted.

[3] D. BLESSENOHL AND K. JOHNSEN, Eine Verschärfung des Satzes von der Normalbasis. *Journal of Algebra* **103** (1986), 141-159.

[4] C.C. FAITH, Extensions of Normal Bases and Completely Basic Fields. *Transactions of the American Mathematical Society* **85** (1957), 406-427.

[5] D. HACHENBERGER, On Completely Free Elements in a Finite Field. *Designs, Codes and Cryptography* **4** (1994), 129-144.

[6] D. HACHENBERGER, Explicit Iterative Constructions of Normal Bases and Completely Free Elements in Finite Fields. *Finite Fields and Their Applications* **2** (1996), 1-20.

[7] D. HACHENBERGER, Normal Bases and Completely Free Elements in Prime Power Extensions over Finite Fields. *Finite Fields and Their Applications* **2** (1996), 21-34.

[8] D. HACHENBERGER, "Finite Fields: Normal Bases and Completely Free Elements." Kluwer Academic Publishers, Boston, 1996, to appear. [1]

[9] N. JACOBSON, "Basic Algebra I. " Freeman and Company, New York, 1985 (2nd Edition).

[10] D. JUNGNICKEL, "Finite Fields. Structure and Arithmetic." Bibliographisches Institut, Mannheim, 1993.

[11] R. LIDL AND H. NIEDERREITER, "Finite Fields." Addison-Wesley, Reading, Massachusetts, 1983.

[12] H. LÜNEBURG, "On the Rational Normal Form of Endomorphisms: A Primer to Constructive Algebra." Bibliographisches Institut, Mannheim, 1987.

[13] O. ORE, Contributions to the Theory of Finite Fields. *Transactions of the American Mathematical Society* **36** (1934), 243-274.

[14] A. SCHEERHORN, Dickson Polynomials and Completely Normal Elements over Finite Fields. *IMA Conference Proceedings Series, Oxford University Press*, to appear.

[15] A. SCHEERHORN, Dickson Polynomials, Completely Normal Polynomials and the Cyclic Module Structure of Specific Extensions of Finite Fields. *Designs, Codes, and Cryptography*, to appear.

Dirk Hachenberger
Institut für Mathematik der Universität Augsburg
Universitätsstraße 14
D-86135 Augsburg
E-mail: Hachenberger@math.uni-augsburg.de

[1] This monograph is based on D. HACHENBERGER, "Normal Bases and Completely Free Elements in Finite Fields." Habilitationsschrift, Mathematisch-Naturwissenschaftliche Fakultät der Universität Augsburg, 1994.