Characterizing Normal Bases via the Trace Map[#]

Dirk Hachenberger*

Institut für Mathematik der Universität Augsburg,
Augsburg, Germany

ABSTRACT

In their recent article Chang et al. [Chang, Y., Troung, T. K., Reed, I. S. (2001). Normal bases over GF(q). *J. Algebra* 241:89–101] have determined all those extensions of Galois fields for which the normal basis generators are characterized by the (obviously necessary) property of having nonzero trace. In the present article, we present a simpler proof of a generalization of that result and discuss an application concerning the existence of trace-compatible sequences of primitive normal bases for certain primary closures of Galois fields.

Key Words: Cyclic Galois extension; Finite (Galois) field; Normal (free) element; Normal basis; Trace; Trace-compatible sequence; Primitive element.

Mathematics Subject Classification: 11T; 12E20.

1. INTRODUCTION

For a finite Galois extension E/F it is well-known that the trace of a normal (or free) element (that is a generator of a normal basis of E/F) is nonzero. In their recent article Chang et al. (2001), have characterized those extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$ of

[#]Communicated by H.-J. Schneider.

*Correspondence: Dirk Hachenberger, Institut für Mathematik der Universität Augsburg, D-86135 Augsburg, Germany; E-mail: hachenberger@math.uni-augsburg.de.

coset $u+M_h$, from which we conclude that

$$(\tau_f^g)^{-1}(M_f') = \bigcup_{u\in M_f'} (u+M_h) = M_f' + M_h.$$

Now, $M_h = \bigcup_{a|h} M_a'$ and $M_f' + M_a' \subseteq M_{fa}'$ by Lemma 2.2 (where $a|h$). Conversely, if $x \in M$ with $\mathrm{ord}(x) = fa$, where f and a are relatively prime, then x can be decomposed into $x_1 + x_2$ with $\mathrm{ord}(x_1) = f$ and $\mathrm{ord}(x_2) = a$ (see Hachenberger, 1997, Theorem 7.3). Thus $M_f' + M_a' = M_{fa}'$ for all $a|h$ and the assertion follows. □

Combining Proposition 2.3 and Proposition 2.4 (including the argument of the proof) with the transitivity (2.2) yields:

Theorem 2.5. *Let f, g be divisors of μ with $f|g$. Write $g = \hat{f}\bar{g}$ where $\bar{g}$ and f are relatively prime, while $\nu(f) = \nu(\hat{f})$. Then*

$$(\tau_f^g)^{-1}(M_f') = \bigcup_{a|\bar{g}} M_{\hat{f}a}' = M_{\hat{f}}' + M_{\bar{g}}.$$

Moreover, if τ_f^g is surjective, then for any $u \in M_f'$ there exists an element $w \in M_g'$ such that $\tau_f^g(w) = u$.

With f and g as in Theorem 2.5, we call $\hat{f}$ the *closure of f in g*. In view of the problem to be addressed in Sec. 3, we note some immediate consequences of Theorem 2.5.

- $(\tau_f^g)^{-1}(M_f') = M_g'$ if and only if $\nu(f) = \nu(g)$ (whence $\hat{f} = g$).
- $(\tau_f^g)^{-1}(M_f') \cap M_f$ is either empty or equal to M_f'; the latter holds if and only if $f = \hat{f}$ (whence f and g/f are relatively prime).
- If $\nu(f) \neq \nu(g)$, then $(\tau_f^g)^{-1}(M_f') \setminus M_f = M_g'$ if and only if g/f is a prime (or irreducible).

3. CHARACTERIZING NORMALITY VIA TRACES

We start this section by recalling some basic facts on the $F[x]$-module structure of a cyclic Galois extension E/F (see Hachenberger, 1997, Sec. 8, for details).

Let n be the degree of E/F and σ a generator of the (cyclic) Galois group of E/F. To each polynomial $g \in F[x]$ there is associated the F-vector-space endomorphism $g(\sigma)$ of E. By defining $w^g := g(\sigma)(w)$ (where $w \in E$) the additive group of E is equipped with an $F[x]$-module structure. As $\sigma^n(w) = w$ for all $w \in E$, the polynomial $\mu = x^n - 1$ annihilates E, whence E is a torsion module. The monic polynomial h of least degree such that $w^h = 0$ is usually called the F-order of w (and denoted by $\mathrm{Ord}_F(w)$). By the famous Normal Basis Theorem (Deuring, 1933; Hensel, 1888; Noether, 1932) there exists an element $u \in E$ such that $\mathrm{Ord}_F(u) = x^n - 1$ (this is equivalent to the fact that

E is cyclic as $F[x]$-module and generated by u, or that $u, \sigma(u), \ldots, \sigma^{n-1}(u)$ is an F-basis of E, i.e., a normal basis of E/F); u is called normal (or free) in E/F.

We may therefore apply the results from Sec. 2 to the present situation (retaining some of the notation introduced there); in particular, the $F[x]$-submodules of E are precisely the sets M_g where $g \in F[x]$ is a monic divisor of $x^n - 1$. Here, the generalized trace-mappings are always surjective; thus, if f and g are monic divisors of $x^n - 1$ such that $f|g$, then for any $u \in M_f'$ there exists a $w \in M_g'$ such that $\tau_f^g(w) = u$ (by Theorem 2.5).

For every divisor k of n, we denote by E_k the unique intermediate field of E/F with degree k over F (whence $E = E_n$). Then $E_k = M_{x^k-1}$, and the mapping τ_f^g where $f = x^k - 1$ and $g = x^n - 1$ is the (E_n, E_k)-trace mapping (which throughout is simply denoted by tr_k^n), i.e.,

$$\mathrm{tr}_k^n : E_n \to E_k, \quad w \mapsto \sum_{j=0}^{\frac{n}{k}-1} \sigma^{kj}(w).$$

Recall that M_{x^n-1}' is the set of normal elements of E/F, while M_{x^k-1}' is the set of normal elements for E_k/F. By Theorem 2.5 we know that every normal element of E_k/F is the trace of some normal element of E_n/F. The aim of the present section is to characterize those triples (F, E_k, E_n), where (essentially) the converse of the latter holds. This leads to a generalization of the main result of Chang et al. (2001) (which concerns the case $k = 1$ for finite fields).

We let $G_{n,k}$ denote the set of $v \in E_n$ satisfying $\mathrm{tr}_k^n(v) \in M_{x^k-1}'$ and $E_k(v) = E_n$.

Theorem 3.1. *Let E/F be a cyclic Galois extension (with generator σ as above) of degree $n > 1$ and k a proper divisor of n. Then the following three assertions are equivalent.*

1. $M_{x^n-1}' = G_{n,k}$.
2. $M_{x^n-1}' = (tr_k^n)^{-1}(M_{x^k-1}') \backslash E_k$.
3. *One of the following two cases occurs:*
   - *F has positive characteristic p, and $\frac{n}{k}$ is a power of p.*
   - *$n = r^l$ and $k = r^{l-1}$ where r is a prime different from the characteristic of F; moreover, the r^lth cyclotomic polynomial Φ_{r^l} is irreducible over F.*

Proof. By definition, $M_{x^n-1}' \subseteq G_{n,k} \subseteq (\mathrm{tr}_k^n)^{-1}(M_{x^k-1}') \backslash E_k$, and therefore (2) implies (1).

Suppose next that (3) holds. If n/k is a power of the characteristic p, say π, then $x^n - 1 = (x^k - 1)^\pi$, whence $\nu(x^k - 1) = \nu(x^n - 1)$, and thus (2) follows from Proposition 2.3. If $n = r^l$ and $k = r^{l-1}$ (with r being a prime different from the characteristic), then $\nu(x^n - 1) \neq \nu(x^k - 1)$ and $(x^n - 1)/(x^k - 1)$ is equal to Φ_{r^l}, the r^lth cyclotomic polynomial. The latter is assumed to be irreducible over F, whence (2) follows from Proposition 2.4. Altogether, this establishes (3) $\Rightarrow$ (2).

We finally prove (1) $\Rightarrow$ (3). For the case where the characteristic p of F is positive, we write $n = \bar{n}\pi(n)$ where $\pi(n)$ is a power of p and $\bar{n}$ is not divisible by p;

similarly write $k=\bar{k}\pi(k)$, and finally let $\pi=\pi(n)/\pi(k)$. Then the closure of x^k-1 in x^n-1 is

$$(x^k-1)^\pi=(x^{\bar{k}}-1)^{\pi(n)}.$$

Furthermore, $x^n-1=(x^k-1)^\pi\cdot\Gamma(x)$, where

$$\Gamma(x):=\prod_{\substack{d\mid\bar{n},\\ d\nmid\bar{k}}}\Phi_d^{\pi(n)}. \tag{3.1}$$

An application of Theorem 2.5 shows that

$$(\mathrm{tr}_k^n)^{-1}(M'_{x^k-1})=\bigcup_{a\mid\Gamma}M'_{(x^k-1)^\pi\cdot a}=M'_{x^{k\pi}-1}+M_\Gamma. \tag{3.2}$$

Observe that n/k is a power of p (i.e., $\bar{k}=\bar{n}$) if and only if $\Gamma=1$ in which case $M'_{x^n-1}=(\mathrm{tr}_k^n)^{-1}(M'_{x^k-1})$. This is consistent with assumption (1) and leads to the first case in (3).

We may therefore assume that n/k has a prime divisor r which is distinct from p. Consider the set $M'_{(x^{k\pi}-1)\Phi_{\bar{n}}}$ (which according to (3.2) is a subset of $(\mathrm{tr}_k^n)^{-1}(M'_{x^k-1})$). The smallest $m\in\mathbb{N}^*$ such that x^m-1 is divisible by $(x^{k\pi}-1)\Phi_{\bar{n}}$ is equal to n, whence $E_k(v)=E_n$ for all v having F-order $(x^k-1)^\pi\Phi_{\bar{n}}$, and this means that $M'_{(x^k-1)^\pi\Phi_{\bar{n}}}$ is a subset of $G_{n,k}$. As $G_{n,k}=M'_{x^n-1}$ by assumption, we obtain $x^n-1=(x^k-1)^\pi\Phi_{\bar{n}}$, and therefore $\Gamma(x)=\Phi_{\bar{n}}$ (because of (3.1)). This in turn implies $\pi(n)=1$ (whence $\pi(k)=1=\pi$, $\bar{k}=k$ and $\bar{n}=n$) and thus $n/k=:r$ is a prime.

If $k=1$, then $n=r$. If $k\neq1$, then $\nu(k)=\nu(n)$, for otherwise Φ_r and Φ_{kr} are distinct divisors of $(x^n-1)/(x^k-1)=\Phi_n$, a contradiction. Let r^l be the maximal power of r dividing n. Now, $\nu(k)=r$, for otherwise there is a prime divisor $s\neq r$ of k, whence Φ_{sr^l} and Φ_{r^l} are distinct divisors of $(x^n-1)/(x^k-1)=\Phi_n$, again a contradiction. We conclude that $n=r^l$ and $k=r^{l-1}$. If Φ_n admits a proper divisor $f\neq1$ in $F[x]$, then any element with F-order $(x^k-1)\cdot f$ is a member of $G_{n,k}$ and therefore $(x^k-1)\cdot f=x^n-1$ by assumption. But this yields $f=\Phi_n$, a further contradiction. This implies the irreducibility of Φ_n over F and finally establishes (1)$\Rightarrow$(3). □

When $k=1$ and E, F are Galois fields, then the equivalence of (1) and (3) of Theorem 3.1 reduces to the main result of Chang et al. (2001) (observe that $l=1$, then).

4. TOWERS OF PRIMITIVE NORMAL BASES

In the present section, we let $F=\mathbb{F}_q$ be the Galois field with q elements and consider an algebraic closure $\hat{F}$ of F. For any $n\in\mathbb{N}^*$ there is exactly one intermediate field E_n of degree n over F (whence E_n is isomorphic of $\mathbb{F}_{q^n}$). Moreover, E_n/F is a cyclic Galois extension whose Galois group is generated by the Frobenius automorphism $\sigma:u\mapsto u^q$. We consider $\hat{F}$ as a torsion module over $F[x]$, where

(analogously to the last section) $w^g = g(\sigma)(w)$ for $w \in \hat{F}$ and $g \in F[x]$. Observe that E_k is contained in E_n if and only if k divides n.

Although the annihilator ideal of $\hat{F}$ is the zero-ideal, the results of Sec. 2 apply to the present situation, when restricting attention to the finite submodules. The finite $F[x]$-submodules of $\hat{F}$ are precisely the sets $M_g = \{v \in \hat{F} : v^g = 0\}$, where $g \in F[x]$ is monic and not divisible by x (this is implicit in Hachenberger, 1997, Chapter II). Moreover, $E_n = M_{x^n-1}$ for all $n \in \mathbb{N}^*$.

In particular, $M'_{x^n-1} \cap (\mathrm{tr}_k^n)^{-1}(M'_{x^k-1})$ is nonempty (whenever $k|n$). Consequently, there exists a sequence $(u_m)_{m\in\mathbb{N}^*}$ such that u_m is normal in $E_{m!}/F$ and $\mathrm{tr}_{(m-1)!}^{m!}(u_m) = u_{m-1}$ for all m (where $m!$ is the factorial of m). Next, for $n \in \mathbb{N}^*$, let $m(n)$ be the least integer such that n divides $m(n)!$, and define $w_n := \mathrm{tr}_n^{m(n)!}(u_{m(n)})$. Then $w_n \in M'_{x^n-1}$ for all n, and the transitivity of the trace mappings implies $\mathrm{tr}_k^n(w_n) = w_k$ whenever k divides n. Due to Scheerhorn (1992), such a sequence $(w_n)_{n\in\mathbb{N}^*}$ is called a *trace-compatible normal sequence for* $\hat{F}/F$; it can in fact be interpreted as a normal basis for the (infinite) algebraic extension $\hat{F}/F$ (see Lenstra, 1985). For the explicit construction of such a sequence, see Hachenberger (1997, Chapter VI).

Recall that a primitive element of a finite field E is a generator of its (cyclic) multiplicative group. We are now going to discuss an interesting application of Theorem 3.1, which in fact includes the generation of the multiplicative group as well, and concerns trace-compatible seuences of *primitive* normal bases for certain primary closures of Galois fields (see Theorem 4.2). We start with a result on primitive normal elements with prescribed trace into an intermediate field.

Theorem 4.1. *Let p be the characteristic of the field $F = \mathbb{F}_q$ and r a prime. Let further $m, l \in \mathbb{N}$ with $m < l$. Assume that $p = r$ or that q is a primitive root modulo r^l. Then the following assertion holds for the triple (F, E_{r^m}, E_{r^l}):*

- *For every $a \in E_{r^m}$ which is normal over F there exists a primitive element $w_a \in E_{r^l}$ such that w_a is normal over F and $\mathrm{tr}_{r^m}^{r^l}(w_a) = a$.*

Proof. First of all, there exists an element $b \in E_{r^{l-1}}$ which is normal over F and has $(E_{r^{l-1}}, E_{r^m})$-trace equal to a (this is an application of Theorem 2.5). Observe next that for a prime r different from the characteristic of F, the r^lth cyclotomic polynomial is irreducible over F if and only if q is a primitive root modulo r^l. Therefore, with $k = r^{l-1}$ and $n = r^l$, the condition (3) of Theorem 3.1 is satisfied, whence any $w \in E_n \backslash E_k$ with (E_n, E_k)-trace equal to b is (already) normal over F. By transitivity, w has (E_n, E_{r^m})-trace equal to a. Now, the assertion follows as Cohen's Theorem on Primitive Elements with Prescribed Trace (Cohen, 1990) (applied to the extension E_n/E_k) asserts that w can be chosen to be a primitive element of E_n. □

If $r = 2$ and q is odd, then Theorem 4.1 applies only to the pairs $(m, l) = (0, 1)$ and $(m, l) = (1, 2)$, where the latter additionally requires that $q \equiv 3$ modulo 4. However, for an *odd* prime r the following three assertions are equivalent by elementary number theory (see e.g. Hachenberger, 1997, Section 19), and therefore allow an iterative application of Theorem 4.1:

- q is a primitive root modulo r^l for all $l \geq 1$.

- q is a primitive root modulo r^2.
- q is a primitive root modulo r and $q^{r-1}-1$ is not divisible by r^2.

For example, $q=2$ is a primitive root modulo r^2 for all the following primes $r \leq 200$: 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197.

Theorem 4.2. *Let p be the characteristic of the field $F=\mathbb{F}_q$ and r a prime such that $r=p$, or such that r is odd and q is a primitive root modulo r^2. Then there exists a sequence $(y_l)_{l\in\mathbb{N}}$ in $E_{r^\infty}:=\bigcup_{l\geq 0}E_{r^l}$ (the r-primary closure of F) satisfying the following two assertions:*

1. *For every l, y_l is a primitive element of E_{r^l} and normal over F.*
2. *For all $l_1 \leq l_2$ the $(E_{r^{l_2}}, E_{r^{l_1}})$-trace of y_{l_2} is equal to y_{l_1}.*

Proof. The assertion follows from Theorem 4.1 by induction and the transitivity of the trace-mappings. □

5. CONCLUDING REMARKS

By Cohen and Hachenberger (1999) the following assertion holds for every extension E/F of Galois fields (and therefore constitutes an improvement of the famous Primitive Normal Basis Theorem of Lenstra and Schoof (1987)):

- For every nonzero $a \in F$ there exists a primitive element $w_a \in E$ which is normal over F and has (E, F)-trace equal to a.

The existence of primitive normal elements with prescribed trace into an intermediate field has first been studied in Hachenberger (1999); using character theory and Gaussian sums it is proved that the conclusion of Theorem 4.2 holds, without any restriction on q, when $r \geq 5$ or $r=p$ (see Hachenberger, 1999, Theorem 6.2). Thus, for $r=3$ and q being a primitive root modulo 9, Theorem 4.2 complements (Hachenberger, 1999, Theorem 6.2). The latter holds for all the following prime powers $q \leq 200$: 2, 5, 11, 23, 29, 32, 41, 47, 59, 83, 101, 113, 128, 131, 137, 149, 167, 173, 191.

A combination of Theorem 4.2 with Hachenberger, (1999, Theorem 6.2) yields the following interesting result which includes the binary field as a ground field.

Theorem 5.1. *Let $q=2^t$ where $\gcd(t, 6)=1$. Let r be any prime. Then there exists a sequence $(y_l)_{l\in\mathbb{N}}$ in the r-primary closure $\mathbb{F}_{q^{r^\infty}}$ over $\mathbb{F}_q$ such that y_l is primitive and normal in $\mathbb{F}_{q^{r^l}}/\mathbb{F}_q$ for all l, and such that the $(\mathbb{F}_{q^{r^{l_2}}}, \mathbb{F}_{q^{r^{l_1}}})$-trace of y_{l_2} is equal to y_{l_1} whenever $l_1 \leq l_2$.*

We finally remark that the results of Sec. 2 may also applied to the multiplicative groups of finite fields, leading in particular to the (relative) *norm*-mappings.

The outcome of Sec. 3 also has consequences for the existence of trace- *and* norm-compatible sequences of primitive normal bases introduced in Hachenberger (2001). We shall develop these lines further in a separate work (see Hachenberger, 2003).

ACKNOWLEDGMENT

The author thanks the referee for valuable suggestions.

REFERENCES

Chang, Y., Troung, T. K., Reed, I. S. (2001). Normal bases over GF(q). *J. Algebra* 241:89–101.

Cohen, S. D. (1990). Primitive elements and polynomials with arbitrary trace. *Discrete Math.* 83:1–7.

Cohen, S. D., Hachenberger, D. (1999). Primitive normal bases with prescribed trace. *Applic. Alg. Engin. Comm. Comp.* 9:383–403.

Deuring, M. (1933). Galoissche Theorie und Darstellungstheorie. *Math. Annalen* 107:180–182.

Fuchs, L. (1960). *Abelian Groups.* 3rd ed. Oxford: Pergamon Press.

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

Hachenberger, D. (1999). Primitive normal bases for towers of field extensions. *Finite Fields Appl.* 5:378–385.

Hachenberger, D. (2001). Universal generators for primary closures of Galois fields. In: Jungnickel, D., Niederreiter, H., eds. Proceedings of the Fifth International Conference on Finite Fields and Applications, Augsburg, August, 1999, Heidelberg, Springer, pp. 208–223.

Hachenberger, D. (2003). Generators for primary closures of Galois fields. *Finite Fields Appl.* 9:122–128.

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

Lenstra, H. W. (1985). A normal basis theorem for infinite Galois extensions. *Indag. Math.* 47:221–228.

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

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

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

Scheerhorn, A. (1992). Trace- and norm-compatible extensions of finite fields. *Applic. Alg. Engin. Comm. Comp.* 3:435–447.

Received August 2002
Revised January 2003