On primitive and free roots in a finite field

Dirk Hachenberger

Angaben zur Veröffentlichung / Publication details:

Hachenberger, Dirk. 1992. “On primitive and free roots in a finite field.” *Applicable Algebra in Engineering, Communications and Computing* 3 (2): 139–50. https://doi.org/10.1007/BF01387196.

On Primitive and Free Roots in a Finite Field

Dirk Hachenberger

Fachbereich Mathematik der Universität Kaiserslautern, Erwin-Schrödinger-Straße, W-6750 Kaiserslautern, Federal Republic of Germany

Received May 22, 1991; revised version July 2, 1991

Abstract. In this paper the m-dimensional extension $\mathbb{F}_{q^m}$ of the finite field $\mathbb{F}_q$ of order q is investigated from an algebraic point of view. Looking upon the additive group $(\mathbb{F}_{q^m}, +)$ as a cyclic module over the principal ideal domain $\mathbb{F}_q[x]$, we introduce a new family of polynomials over $\mathbb{F}_q$ which are the additive analogues of the cyclotomic polynomials. Two methods to calculate these polynomials are proposed. In combination with algorithms to compute cyclotomic polynomials, we obtain, at least theoretically, a method to determine all elements in $\mathbb{F}_{q^m}$ of a given additive and multiplicative order; especially the generators of both cyclic structures, namely the generators of primitive normal bases in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, are characterized as the set of roots of a certain polynomial over $\mathbb{F}_q$.

Keywords: Finite field, Primitive root, Free root, Normal basis, Primitive normal basis, Cyclotomic polynomial, π-polynomial

Introduction

Let $q > 1$ be a prime power, $\mathbb{F}_q$ the finite field of order q and $\mathbb{F}_q[x]$ the ring of polynomials over $\mathbb{F}_q$ in the indeterminate x. The m-dimensional extension $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is a Galois extension with cyclic Galois group of order m which is generated by the *Frobenius automorphism* $\sigma: \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, $\alpha \to \alpha^q$.

Being a cyclic group of order $q^m - 1$, the multiplicative group $(\mathbb{F}_{q^m}^*, \cdot)$ is a cyclic $\mathbb{Z}$-module and its generators are the *primitive roots* of $\mathbb{F}_{q^m}$. In [3] these elements are called *primitive roots of the first kind.*

A *normal basis* of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is a basis of the form $(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}})$. α is called a *free root* in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It is well known that there always do exist normal bases in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ (see e.g. [6, 10]). In [10] all quoted facts concerning finite fields may be found. Generators of normal bases are called *primitive roots of the second kind* in [3].

The following result has its origin in O. Ore's publications [14] and [15]. It is also dealt with in the papers [3], [5] and [9], being an essential aspect which shows that the multiplicative and additive groups of the extension $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are very similar.

(1.1) Theorem. *Let $f := \sum_{i=0}^{n} f_i x^i$ be a polynomial of $\mathbb{F}_q[x]$ and let $\alpha \in \mathbb{F}_{q^m}$. The scalar multiplication $\circ : \mathbb{F}_q[x] \times \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$,*

$$(f, \alpha) \to f \circ \alpha := \sum_{i=0}^{n} f_i \alpha^{q^i}$$

turns the additive group $(\mathbb{F}_{q^m}, +)$ into a finite, cyclic module over $\mathbb{F}_q[x]$, its generators are exactly the free roots in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

We introduce the following notation (c.f. [14], [15] and [9]):

(1.2) Definitions.

(i) *The kernel of the mapping $\Psi_\alpha : \mathbb{F}_q[x] \to \mathbb{F}_{q^m}$, $f \to f \circ \alpha$ is called the annihilator ideal of α; the monic generator of kernel(Ψ_α) is called the additive order of α over $\mathbb{F}_q$.*

(ii) *The polynomial $F := \sum_{i=0}^{n} f_i x^{q^i}$ of $\mathbb{F}_q[x]$ is called the associated q-polynomial of $f := \sum_{i=0}^{n} f_i x^i$.*

The generators of the two cyclic module structures are very important for representing and computing the elements of finite fields. Therefore they have an essential role in applications, e.g. coding theory or cryptography (see e.g. [1], [2], [10], [11], [13]).

In order to keep this paper self-contained, we will prove some results on finite cyclic modules over principal ideal domains in Sect. 2. The application of these facts to finite fields will imply some known theorems from [9] and [10].

In [3], [5] and [9] advantage is taken of the analogy of both group structures in $\mathbb{F}_{q^m}$ (regarding certain principal ideal domains) to apply the *Vinogradov criterion*, a sufficient condition for primitive roots (see [8]; also used in [4] and [7]) to the additive group $(\mathbb{F}_{q^m}, +)$. Consequently one obtains a sufficient condition for free roots. Both conditions (Vinogradov criterion and the additive analogue) are fundamentally important for the proof of

(1.3) Theorem (Lenstra and Schoof [9]). *For every prime power $q > 1$ and every positive integer $m > 1$ there exists a primitive normal basis in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, i.e. a normal basis which is generated by a primitive root.*

In this paper further known results on cyclic groups will be applied to $(\mathbb{F}_{q^m}, +)$ as a module over $\mathbb{F}_q[x]$: In Sect. 3, generalizing the *cyclotomic polynomials*, we will obtain a new class of polynomials over $\mathbb{F}_q[x]$ which we have called *π-polynomials*. The roots of a π-polynomial are exactly the elements in $\mathbb{F}_{q^m}$ of a given *additive order* over $\mathbb{F}_q$. By using the Möbius inversion formula we obtain an explicit representation for π-polynomials. As this representation is merely of theoretical interest, we discuss a recursive algorithm to calculate π-polynomials in Sect. 4. This algorithm is the analogue of the already known method to compute cyclotomic polynomials over the field of rational numbers quickly (c.f. [11]).

Theorem (1.3) says that the $(q^m - 1)$th cyclotomic polynomial in $\mathbb{F}_q[x]$ and the π-polynomial, whose roots are the free roots in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, have a greatest common divisor of degree greater than 0. This is the polynomial with roots being exactly the generators of primitive normal bases. The algorithms mentioned above in combination with the Euclidean algorithm in particular give at least a theoretical method to compute this (in most cases pure) nontrivial factor of the (q^m-1)th cyclotomic polynomial and consequently a method to calculate primitive (and free) roots in general.

2. Finite, Cyclic Models over Principal Ideal Domains

In this section M denotes a finite, cyclic module over a principal ideal domain R satisfying $|R| = \infty$. We first introduce some notation:

For an element α of M let $\langle\alpha\rangle := \{r\alpha : r \in R\}$ be the R-submodule of M generated by α. $\mathrm{Ann}_R(\alpha) := \{r \in R : r\alpha = 0\}$ denotes the annihilator ideal of α. The generator $\mathrm{Ord}_R(\alpha)$ of $\mathrm{Ann}_R(\alpha)$ is called the *R-order of α*. The generator of $\mathrm{Ann}_R(M) := \{r \in R : r\alpha = 0$ for all $\alpha \in M\}$ is denoted by $\mathrm{Ord}_R(M)$.

$\mathrm{Ord}_R(\alpha)$ and $\mathrm{Ord}_R(M)$ are uniquely determined modulo the group of units in R. Being a module over R, $\langle\alpha\rangle$ is isomorphic to the factor module $R/\mathrm{Ann}_R(\alpha)$.

As we are only interested in ring elements of the form $r = \mathrm{Ord}_R(\zeta)$ for a suitable $\zeta \in M$, we may assume, without loss of generality, that $R/(r)$ is finite for all $r \in R - \{0\}$. (Here (r) denotes the ideal generated by r). Let $\Phi_R(r)$ denote the number of generators of the module $R/(r)$.

To be able to determine $\Phi_R(r)$ for all $r \in R - \{0\}$, we first list some elementary properties which can be found in many algebra books (e.g. [6], [12]).

(2.1) Lemma.
(i) *Let r be an element of $R - \{0\}$. The generators of the R-module $R/(r)$ are exactly the units of the ring $R/(r)$.*
(ii) *Let $a, b \in R - \{0\}$, then* $\gcd(a,b) = 1$ *if-and only if $a + (b)$ is a unit in $R/(b)$.*
(iii) *Chinese remainder theorem: Let $a_1, \dots, a_n$ be elements of $R - \{0\}$ satisfying* $\gcd(a_i, a_j) = 1$ *for all $i \neq j$. Then for every n-tuple $(b_1, \dots, b_n)$ in R^n there exists an $x \in R$, such that $x \equiv b_i \bmod (a_i)$ for all $i = 1, \dots, n$. Moreover, x is uniquely determined modulo $(a_1 \cdot \dots \cdot a_n)$.*

We are now able to compute $\Phi_R(r)$ for all $r \in R - \{0\}$ by using the prime decomposition of r in R.

(2.2) Theorem.
(i) $\Phi_R(a) = 1$ *if and only if a is a unit in R.*
(ii) *Let $a, b \in R - \{0\}$ with* $\gcd(a,b) = 1$, *then* $\Phi_R(ab) = \Phi_R(a) \cdot \Phi_R(b)$.
(iii) *If $a = p^k$ where $k \geqq 1$ and p is irreducible in R, then* $\Phi_R(a) = |R/(p^k)| - |R/(p^{k-1})|$.
(iv) *Let $\prod_{i=1}^{t} p_i^{k_i}$ be the prime decomposition of $a \in R - \{0\}$,* $\gcd(p_i, p_j) = 1$ *for $i \neq j$ and $k_i \geqq 1$ for all i. Then* $\Phi_R(a) = \prod_{i=1}^{t} (|R/(p_i^{k_i})| - |R/(p_i^{k_i-1})|)$.

Proof.
(i) follows immediately from (2.1)(i) and the definition of Φ_R.
(ii) is an application of (2.1)(ii) and (iii):

By using (2.1)(ii) it is easy to see that the element $x+(ab)$ is a unit in $R/(ab)$ if and only if $x+(a)$ and $x+(b)$ are units in $R/(a)$ and $R/(b)$ respectively.

Conversely, let $(u+(a), v+(b))$ be a pair of units of $R/(a) \times R/(b)$. According to (2.1)(iii) there exists a unique element y modulo $a \cdot b$ satisfying $y \equiv u \bmod a$ and $y \equiv v \bmod a$. Hence $y+(a)$ and $y+(b)$ are units in $R/(a)$ and $R/(b)$ respectively.
(iii) follows from (2.1)(ii) since the elements $a+(p^k)$ of $R/(p^k)$ divided by $p+(p^k)$ are in one-to-one correspondence with the elements of $R/(p^{k-1})$.
(iv) follows by induction from (ii) and (iii). □

The next result is a generalization of the structure theorem on finite cyclic groups in [6]. We skip the easy proof.

(2.3) Theorem. *Let* $A := \mathrm{Ord}_R(M)$, *then*:
(i) *Every* R*-submodule* N *of* M *is cyclic and* $\mathrm{Ord}_R(N)$ *is a divisor of* A.
(ii) *Modulo the group of units in* R, *for every divisor* r *of* A *there exists exactly one* R*-submodule* U_r *of* M *satisfying* $\mathrm{Ord}_R(U_r) = r$.
(iii) *For every divisor* r *of* A *there are exactly* $\Phi_R(r)$ *elements of* R*-order* r *in* M *Moreover, one has*

$$\sum_{r|A} \Phi_R(r) = |M| = |R/(A)|$$

where r *runs over a complete system of pairwise non-associate divisors of* A.

By applying (2.2) to the cyclic module structures in finite fields, we obtain some well known results:

For $\alpha \in \mathbb{F}_{q^m}^*$ let $\mathrm{ord}(\alpha) := \mathrm{Ord}_{\mathbb{Z}}(\alpha) = \min\{n \in \mathbb{N} : \alpha^n = 1\}$ be the *multiplicative order of* α. According to (2.1) the number of primitive roots in $\mathbb{F}_{q^m}^*$ is equal to the number of units in the ring $\mathbb{Z}/(q^m-1)\mathbb{Z}$, hence $\Phi_{\mathbb{Z}} =: \varphi$ is the well known *Euler-function* from number theory. Furthermore, (2.2) yields

(2.4) Corollary. *Let* a *be a divisor of* $q^m - 1$. *Then the number of elements of order* a *in* $\mathbb{F}_{q^m}^*$ *is equal to*

$$\varphi(a) = \prod_{i=1}^{k} (|\mathbb{Z}_{p_i^{l_i}}| - |\mathbb{Z}_{p_i^{l_i-1}}|) = a \cdot \prod_{i=1}^{k} (1 - p_i^{-1})$$

where $\prod_{i=1}^{k} p_i^{l_i}$ *is the prime decomposition of* a. *In particular* $\varphi(q^m-1)$ *is the number of primitive roots in* $\mathbb{F}_{q^m}$.

We are now going to investigate the additive group $(\mathbb{F}_{q^m}, +)$ as cyclic module over $\mathbb{F}_q[x]$ and will again obtain some known facts (see [10, Chap. 3.4] and [9]).

Let $\mathrm{Ord}(\beta) := \mathrm{Ord}_{\mathbb{F}_q[x]}(\beta)$ denote the *additive order of* β. According to (1.2) (i) this is the monic polynomial of least degree satisfying $g \circ \beta = 0$. Furthermore, let $\Phi_q := \Phi_{\mathbb{F}_q[x]}$.

As the group of units in $\mathbb{F}_q[x]$ is isomorphic to $\mathbb{F}_q^*$ and as $\mathrm{Ord}(\mathbb{F}_{q^m}) = x^m - 1$, the additive orders of elements in $\mathbb{F}_{q^m}$ correspond to the monic divisors of $x^m - 1$ in $\mathbb{F}_q[x]$. We obtain

(2.5) Corollary. *Let* f *be a monic divisor of* $x^m - 1$ *in* $\mathbb{F}_q[x]$ *with prime decomposition* $f_1^{k_1} \cdot f_2^{k_2} \cdot \ldots \cdot f_n^{k_n}$. *Then the number of elements in* $\mathbb{F}_{q^m}$ *which have additive order* f *over*

$\mathbb{F}_q$ *is equal to*

$$\Phi_q(f) = \prod_{i=1}^{n} (|\mathbb{F}_q[x]/(f_i^{k_i})| - |\mathbb{F}_q[x]/(f_i^{k_i-1})|) = q^{\deg f} \prod_{i=1}^{n} (1 - q^{-\deg f_i}).$$

(Here $\deg f$ *denotes the degree of* f.*)*

We close this section with the Möbius inversion formula (c.f. [6]) which will be applied in Sect. 3.

(2.6) Theorem (Möbius inversion formula). *Let* h *and* H *be two mappings of* R *into a (multiplicatively written) abelian group* G. *Then for every* $b \in R - \{0\}$

$$H(b) = \prod_{r|b} h(r) \text{ if and only if } h(b) = \prod_{r|b} H(r)^{\mu_R(b/r)}$$

where

$$\mu_R(a) := \begin{cases} 1, & \text{if } a \text{ is a unit in } R \\ 0, & \text{if } a \text{ is not square-free} \\ (-1)^k, & \text{otherwise, with } k \text{ denoting the number of distinct irreducible divisors of } a \end{cases}$$

is the Möbius function in R *(with* r *as in (2.3)* (iii) *running over a complete system of pairwise non-associate divisors of* b*).*

3. A Characterization of the Elements in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$

The algebraic structure of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ essentially depends on the following three facts.

(1) The divisors of m are in one-to-one correspondence with the fields that lie between $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$. The *degree* $\deg(\alpha)$ of the minimal polynomial of $\alpha \in \mathbb{F}_{q^m}$ is a divisor of m and the field generated by $\mathbb{F}_q$ and α is equal to $\mathbb{F}_{q^s}$ where $s = \deg(\alpha)$. Thus α is called a *defining element* of $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$.

(2) The divisors of $q^m - 1$ by (2.3) are in one-to-one correspondence with the subgroups of $\mathbb{F}_{q^m}^*$. Every α in $\mathbb{F}_{q^m}^*$ has a multiplicative order $\operatorname{ord}(\alpha)$ which is a positive divisor of $q^m - 1$.

(3) The monic divisors of the polynomial $x^m - 1$ in $\mathbb{F}_q[x]$ by (2.3) are in one-to-one correspondence with the $\mathbb{F}_q[x]$- submodules of $\mathbb{F}_{q^m}$. Every $\alpha \in \mathbb{F}_{q^m}$ has an additive order $\operatorname{Ord}(\alpha)$ which is a monic divisor of $x^m - 1$.

Therefore the role of α in $\mathbb{F}_{q^m}$ is described by the triple $(\deg(\alpha), \operatorname{ord}(\alpha), \operatorname{Ord}(\alpha))$. We define $\operatorname{ord}(0) := \infty$. The following Lemma (3.2) (c.f. [9]) shows that the degree of α is already specified by the quantities $\operatorname{ord}(\alpha)$ and $\operatorname{Ord}(\alpha)$ respectively. First some notation is required.

(3.1) Notation. Let a be a positive divisor of $q^m - 1$ and f a monic divisor of $x^m - 1$ in $\mathbb{F}_q[x]$. We denote by $\operatorname{ord}_a(q) := \min\{k \in \mathbb{N} : q^k \equiv 1 \bmod a\}$ the multiplicative order of q in the group of units of $\mathbb{Z}/a\mathbb{Z}$ and by $\operatorname{Ord}_f(x) := \min\{k \in \mathbb{N} : x^k \equiv 1 \bmod f\}$

the multiplicative order of x in the group of units of $\mathbb{F}_q[x]/(f)$ respectively. (Because of $\gcd(a,q)=1$ and $\gcd(f,x)=1$ these terms are well-defined.)

(3.2) Lemma. *Let* $\alpha\in\mathbb{F}^*_{q^m}, a:=\operatorname{ord}(\alpha)$ *and* $f:=\operatorname{Ord}(\alpha)$. *Then* $\deg(\alpha)=\operatorname{ord}_a(q)=\operatorname{Ord}_f(x)$.

Proof. If $d=\operatorname{ord}_a(q)$, then by definition d is the smallest positive integer satisfying $a|q^d-1$. Consequently α is a defining element of $\mathbb{F}_{q^d}$ and $\deg(\alpha)$ is equal to d.

If $e=\operatorname{Ord}_f(x)$, then by definition e is the smallest positive integer satisfying $f|x^e-1$ and therefore minimal with $(x^e-1)\circ\alpha=\alpha^{q^e}-\alpha=0$. So $\langle\sigma^e\rangle$ is the Galois-group over $\langle\mathbb{F}_q,\alpha\rangle$, the field generated by $\mathbb{F}_q$ and α (as in the first section, σ denotes the Frobenius-automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$). This also yields $e=\deg(\alpha)$. □

After having proved that α is characterized by the pair $(\operatorname{ord}(\alpha),\operatorname{Ord}(\alpha))$, we are now going to discuss a problem L. Carlitz partially has dealt with in [3].

(3.3) Problem. Let (a,f) be a pair with $a|q^m-1, f|x^m-1$ (f monic). Do there exist elements α in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ with $\operatorname{ord}(\alpha)=a$ and $\operatorname{Ord}(\alpha)=f$?

Lemma (3.2) yields a necessary condition on the pair and therefore shows that (3.3) cannot hold in general. We call a pair (a,f) satisfying $\operatorname{ord}_a(q)=\operatorname{Ord}_f(x)$ a *nontrivial* one.

Theorem (1.3) of Lenstra and Schoof implies that there always exist elements of the *type* (q^m-1,x^m-1) in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

In this section we want to show, how at least theoretically one can compute all primitive *and* free roots (generators of primitive normal bases) in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and, more generally, all elements of a given nontrivial type (a,f). We are therefore going to introduce a new family of polynomials, being the additive analogues of the cyclotomic polynomials.

(3.4) Notation and definition.

(i) For a divisor a of q^m-1 let

$$B_a:=\{\alpha\in\mathbb{F}_{q^m}:\operatorname{ord}(\alpha)=a\}\quad\text{and}\quad Q(a;x):=\prod_{\beta\in B_a}(x-\beta).$$

$Q(a;x)$ is called the *ath cyclotomic polynomial* in $\mathbb{F}_q[x]$.

(ii) For a monic divisor f of x^m-1 in $\mathbb{F}_q[x]$ let

$$A_f:=\{\alpha\in\mathbb{F}_{q^m}:\operatorname{Ord}(\alpha)=f\}\quad\text{and}\quad P(f;x):=\prod_{\beta\in A_f}(x-\beta).$$

We call $P(f;x)$ the *π-polynomial over $\mathbb{F}_q$ belonging to f.*

Next we state a well known theorem which is proved in [10] by applying the Möbius inversion formula.

(3.5) Theorem. *Let a be a divisor of q^m-1. The polynomial $Q(a;x)$ is an element of $\mathbb{F}_q[x]$. It splits in $\mathbb{F}_q[x]$ into the product of $\dfrac{\varphi(a)}{\operatorname{ord}_a(q)}$ factors of degree $\varphi(a)$ and satisfies*

$$Q(a;x)=\prod_{d|a}(x^d-1)^{\mu(a/d)}$$

where μ denotes the Möbius function in $\mathbb{Z}$.

Similarly, considering the additive group $(\mathbb{F}_{q^m}, +)$ as an $\mathbb{F}_q[x]$ – module, one gets the following result:

(3.6) Theorem. *Let f be a monic divisor of $x^m - 1$ in $\mathbb{F}_q[x]$. The polynomial $P(f;x)$ is an element of $\mathbb{F}_q[x]$.*

It splits in $\mathbb{F}_q[x]$ into the product of $\dfrac{\Phi_q(f)}{\mathrm{Ord}_f(x)}$ irreducible polynomials of degree $\mathrm{Ord}_f(x)$ and satisfies

$$P(f;x) = \prod_{\substack{e|f \\ e \text{ monic}}} E(x)^{\mu_q(f/e)}$$

where E denotes the associated q-polynomial belonging to e (see (1.2) (iii)) and μ_q denotes the Möbius function in the ring $\mathbb{F}_q[x]$.

Proof. Because of $\gcd(x, x^m - 1) = 1$ the polynomial x is a unit in $\mathbb{F}_q[x]/(x^m - 1)$ and therefore induces with $\alpha \to x \circ \alpha = \alpha^q$ an $\mathbb{F}_q[x]$-module automorphism on $\mathbb{F}_{q^m}$. For this reason the conjugates of α have the same additive order as α. Hence, for any monic divisor f of $x^m - 1$, the set $A_f = \{\alpha \in \mathbb{F}_{q^m} | \mathrm{Ord}(\alpha) = f\}$ is a union of classes of conjugate elements and therefore being a product of irreducible polynomials in $\mathbb{F}_q[x]$, $P(f;x)$ itself is a member of $\mathbb{F}_q[x]$.

The second assertion follows immediately from the facts that the number of elements of A_f is equal to $\Phi_q(f)$ (see (2.3)) and that the number of elements in every conjugacy class in A_f is equal to $\mathrm{Ord}_f(x)$ (see (3.2)).

By using the ring $\mathbb{F}_q[x]$, the group $(\{fg^{-1} : f, g \in \mathbb{F}_q[x] - \{0\}, \cdot)$ and the formula

$$x^{q^m} - x = \prod_{\substack{f|x^m - 1 \\ f \text{ monic}}} \prod_{\beta \in A_f} (x - \beta) = \prod_{\substack{f\ x^m - 1 \\ f \text{ monic}}} P(f;x),$$

we finally may deduce the representation of $P(f;x)$ from (2.3) and (2.6).

For every monic divisor f of $x^m - 1$ in $\mathbb{F}_q[x]$ we set $h(f) := P(f;x)$. Furthermore, let $U_f := \{\alpha \in \mathbb{F}_{q^m} : f \circ \alpha = 0\}$ denote the unique submodule of $\mathbb{F}_{q^m}$ belonging to f. By definition the elements of U_f have an additive order dividing f and therefore coincide with the set of roots of the polynomials $P(e;x)$ where e is a monic divisor of f in $\mathbb{F}_q[x]$.

On the other hand, every element α of order e dividing f lies in U_f, whence U_f is exactly the set of roots of the associated q-polynomial F of f (c.f. (1.2) (ii)). We therefore obtain

$$\prod_{\substack{e\ f \\ e \text{ monic}}} P(e;x) = \prod_{\beta \in U_f} (x - \beta) = F(x).$$

Setting $H(f) := F$ and using the Möbius inversion formula (2.6), we obtain the desired representation of $P(f;x)$. □

The following theorem is a direct consequence of (3.5), (3.6) and (3.2).

(3.7) Theorem. *Let (a, f) be a nontrivial pair belonging to $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

(i) *The intersection $A_f \cap B_a$ is exactly the set of elements in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ having multiplicative order a and additive order f.*

(ii) *This set consists exactly of the roots of the polynomial* $R(a, f; x) := \gcd(Q(a; x), P(f; x))$.
$A_f \cap B_a$ is non-empty if and only if $R(a, f; x) \neq 1$.

(iii) *$A_f \cap B_a$ is a union of classes of conjugate elements with respect to the Galois group of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

(iv) *The cardinality of $A_f \cap B_a$ is a multiple of* $\operatorname{Ord}_f(x) = \operatorname{ord}_a(q)$.

In our notation, Theorem (1.3) of Lenstra and Schoof may now be stated as follows:

(3.8) Theorem. *For every prime power $q > 1$ and every positive integer $m > 1$ the greatest common divisor $R(q^m - 1, x^m - 1; x)$ of $Q(q^m - 1; x)$ and $P(x^m - 1; x)$ has degree greater than 0.*

We close this section with some examples which among other things show that there do exist field extensions with nontrivial pairs (a, f) satisfying $|A_f \cap B_a| = 0$. Therefore Theorem (1.3) cannot be generalized to all nontrivial pairs.

(3.9) Example. We investigate the extension $\mathbb{F}_{16}$ over $\mathbb{F}_2$ and first calculate all primitive normal bases with (3.5), (3.6) and (3.7).

Because of $2^4 - 1 = 3 \cdot 5$ and $x^4 - 1 = (x - 1)^4$ we obtain

$$P(x^4 - 1; x) = x^8 + x^4 + x^2 + x + 1 = (x^4 + x^3 + 1) \cdot (x^4 + x^3 + x^2 + x + 1)$$

and

$$Q(15; x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 = (x^4 + x^3 + 1) \cdot (x^4 + x + 1).$$

The greatest common divisor of these polynomials is $x^4 + x^3 + 1$, hence there exist exactly four elements which are primitive *and* free in $\mathbb{F}_{16}$ over $\mathbb{F}_2$.

In the Table 1 we have listed all irreducible polynomials of degree 1, 2 or 4 in $\mathbb{F}_2[x]$ with corresponding multiplicative and additive orders of their roots. Examining all non-trivial pairs, we see that there are no elements of the type $(5, x^3 + x^2 + x + 1)$.

Table 1

Root of	Mult. order	Additive order
$x^4 + x^3 + 1$	15	$x^4 - 1$
$x^4 + x^3 + x^2 + x + 1$	5	$x^4 - 1$
$x^4 + x + 1$	15	$x^3 + x^2 + x + 1$
$x^2 + x + 1$	3	$x^2 + 1$
$x + 1$	1	$x - 1$
x	∞	1

(3.10) Example. Let $q > 1$ be any odd prime power and let $m = 2$.

Then $x^2 - 1 = (x - 1)(x + 1)$. Any defining element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ has additive order $x + 1$ or $x^2 + 1$. (Note that $x - 1$ is different from $x + 1$ as $\mathbb{F}_q$ by assumption has odd characteristic.) Let α be a primitive root of $\mathbb{F}_{q^2}^*$. If $(x + 1) \circ \alpha = \alpha^q + \alpha = 0$, then $\alpha^{q-1} = -1$, whence $\operatorname{ord}(\alpha) = q^2 - 1$ is a divisor of $2q - 2$. This is a contradiction and we obtain that there do not exist elements in $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ of nontrivial type $(q^2 - 1, x + 1)$.

Consequently, any primitive root in $\mathbb{F}_{q^2}$ is a free root over $\mathbb{F}_q$.

4. A Recursive Method for Calculating π-Polynomials

In H. Lüneburg [11, §14] a quick method to compute cyclotomic polynomials over the field of rational numbers is presented. In this section, advantage will be taken of a similar strategy to describe how π-polynomials can be calculated recursively.

If f is a monic divisor of $x^m - 1$ in $\mathbb{F}_q[x]$, we will call an element α of A_f (c.f. (3.4) (ii)) a *generating root of f*. Furthermore we denote by P_f the π-polynomial $P(f;x)$. By defining

$$(f \odot g)(x) := f(G(x))$$

we introduce a new multiplication in $\mathbb{F}_q[x]$ (again G denotes the associated q-polynomial belonging to g).

(4.1) Lemma. *Let f and g be monic divisors of $x^m - 1$ such that $fg \mid x^m - 1$. Then P_{fg} is a divisor of $P_f \odot g$.*

Proof. By definition the roots of P_{fg} are exactly the generating roots of fg. We therefore have to show that α is also a root of $P_f \odot g$ for any α in A_{fg}:

Because of the fact that $\operatorname{Ord}(\alpha) = fg$, the element $g \circ \alpha$ is a generating root of f and consequently a root of P_f. The definition of $\circ$ in (1.1) yields $P_f(g \circ \alpha) = P_f(G(\alpha)) = (P_f \odot g)(\alpha)$. □

The recursive calculation of π-polynomials is essentially based on the following results (4.2) and (4.3).

(4.2) Theorem. *Let f be a proper monic divisor of $x^m - 1$ and g be an irreducible divisor of $x^m - 1$ in $\mathbb{F}_q[x]$ satisfying* $\gcd(f, g) = 1$.

Then fg is a divisor of $x^m - 1$ and one has $P_f P_{fg} = P_f \odot g$.

Proof. Let β be a root of P_f. That means $\operatorname{Ord}(\beta) = f$. By assumption we have $\gcd(f, g) = 1$. Hence g induces with $\alpha \to g \circ \alpha$ an $\mathbb{F}_q[x]$-module – automorphism on the submodule $U_f = \{\alpha \in \mathbb{F}_{q^m} \mid f \circ \alpha = 0\}$ and therefore in particular a bijection on the set A_f of generating roots of f. This shows that $g \circ \beta$ is also a root of P_f. Thus $0 = P_f(g \circ \beta) = P_f(G(\beta)) = (P_f \odot g)(\beta)$ and therefore P_f divides $P_f \odot g$.

As P_f and P_{fg} are relatively prime, together with (4.1) we obtain that likewise their product is a divisor of $P_f \odot g$. As $P_f P_{fg}$ and $P_f \odot g$ are monic polynomials, now it suffices to show that their degrees are equal.

With (2.1), (2.2), the assumption that f and g are relatively prime and the fact that $\deg(P_f) = |A_f| = \Phi_q(f)$, one gets

$$\deg(P_{fg} P_f) = \Phi_q(fg) + \Phi_q(f) = \Phi_q(f)\Phi_q(g) + \Phi_q(f) = \Phi_q(f)(\Phi_q(g) + 1).$$

Furthermore, considering that g is irreducible, with (2.2) (iii) we obtain $\Phi_q(g) = q^{\deg(g)} - 1$ and therefore

$$\deg(P_{fg} P_f) = \Phi_q(f) q^{\deg(g)}.$$

On the other hand, according to $\deg(G) = q^{\deg(g)}$ and the definition of $\odot$, we have

$$\deg(P_f \odot g) = \deg(P_f) \cdot \deg(G) = \Phi_q(f) q^{\deg(g)}.$$

This proves (4.2). □

(4.3) Theorem. *Let f, g and fg be monic divisors of $x^m - 1$.*

If every irreducible divisor of g is a divisor of f, one has $P_{fg} = P_f \odot g$.

Proof. According to (4.1) the polynomial P_{fg} is a divisor of $P_f \odot g$. As both polynomials are monic, it again suffices to prove the equality of their degrees. We have (see also the proof of (4.2))

$$\deg(P_f \odot g) = \Phi_q(f) q^{\deg(g)}.$$

Furthermore, by (2.3), (2.5) in connection with (3.4) (ii) and the assumptions on f and g we have

$$\deg(P_{fg}) = \Phi_q(fg) = q^{\deg(fg)} \prod_{\substack{h|fg \\ h \text{ irred.}}} (1 - q^{-\deg(h)})$$
$$= q^{\deg(f)} q^{\deg(g)} \prod_{\substack{h|f \\ h \text{ irred.}}} (1 - q^{-\deg(h)}) = \Phi_q(f) q^{\deg(g)}.$$

This proves (4.3). □

Now let f be a monic divisor of $x^m - 1$ over $\mathbb{F}_q[x]$. The following procedure shows, how to obtain P_f by applying (4.2) and (4.3), provided that the prime decomposition of f is given.

If f has no multiple roots which is valid in any case, provided that the characteristic of $\mathbb{F}_q$ does not divide m, we calculate P_f with the help of (4.2). Let $f_1 f_2 \ldots f_t$ be the decomposition of f into irreducible polynomials in $\mathbb{F}_q[x]$. By (3.6) one gets

$$P_{f_1} = F_1(x) \cdot x^{-1}.$$

(F_1 is the associated q-polynomial of f_1.)

In the case $t = 1$ we have finished. Otherwise f_1 and f_2 satisfy the assumptions of (4.2) which yields $P_{f_1} P_{f_1 f_2} = P_{f_1} \odot f_2$ and therefore

$$P_{f_1 f_2} = (P_{f_1} \odot f_2) P_{f_1}^{-1}.$$

Recursively we obtain

$$P_{f_1 f_2 \cdots f_{t-1}} P_{f_1 f_2 \cdots f_t} = P_{f_1 f_2 \cdots f_{t-1}} \odot f_t$$

and therefore

$$P_f = P_{f_1 f_2 \cdots f_t} = (P_{f_1 f_2 \cdots f_{t-1}} \odot f_t) P_{f_1 f_2 \cdots f_{t-1}}^{-1}.$$

If f has multiple roots, e.g. $f = \tau(f) g$ where $\tau(f)$ is the square-free part of f, we use the above algorithm to determine $P_{\tau(f)}$ and then use (4.3) to calculate P_f by

$$P_f = P_{\tau(f) g} = P_{\tau(f)} \odot g.$$

(4.4) Example. Let $q = 2$ and $m = 6$. We want to determine all primitive and free roots in $\mathbb{F}_{64}$ over $\mathbb{F}_2$.

1. Step – (Determination of $Q_{63}(x) := Q(63; x)$, the 63rd cyclotomic polynomial over $\mathbb{F}_2$):

We use the algorithm in [11, §14].

(1a) $63 = 3^2 \cdot 7$.

(1b) $Q_3(x) = x^2 + x + 1$.

(1c) $$Q_{21}(x) = Q_{3\cdot 7}(x) = Q_3(x^7)\cdot Q_3(x)^{-1}$$
$$= x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1.$$

(1d) $$Q_{63}(x) = Q_{21}(x^3)$$
$$= x^{36} + x^{33} + x^{27} + x^{24} + x^{18} + x^{12} + x^9 + x^3 + 1.$$

2. *Step* – (Determination of P_{x^6-1}):
We use the algorithm above.

(2a) $$x^6 - 1 = (x+1)^2(x^2+x+1)^2 \text{ over } \mathbb{F}_2.$$

(2b) $$P_{x+1} = (x^2+x)\cdot x^{-1} = x+1.$$

(2c) $$P_{x^3+1} = P_{(x+1)\cdot(x^2+x+1)} = ((x+1)\odot(x^2+x+1))\cdot(x+1)^{-1}$$
$$= (x^4+x^2+x+1)\cdot(x+1)^{-1} = x^3+x^2+1.$$

(2d) $$P_{x^6-1} = (x^3+x^2+1)\odot(x^3+1) = (x^8+x)^3 + (x^8+x)^2 + 1$$
$$= x^{24} + x^{17} + x^{16} + x^{10} + x^3 + x^2 + 1.$$

3. *Step*
Determination of $\gcd(Q_{63}, P_{x^6-1})$ with the Euclidean algorithm yields

$$\gcd(Q_{63}, P_{x^6+1}) = x^{18} + x^{17} + x^{15} + x^{12} + x^9 + x^7 + x^4 + x^3 + 1.$$

4. *Step*
Factorization of this polynomial over $\mathbb{F}_2$ gives

$$\gcd(Q_{63}, P_{x^6+1}) = (x^6+x^5+1)\cdot(x^6+x^5+x^2+x+1)\cdot(x^6+x^5+x^4+x+1).$$

We obtain that there are exactly 18 primitive *and* free roots in $\mathbb{F}_{64}$ over $\mathbb{F}_2$. The corresponding minimal polynomials are (x^6+x^5+1), $(x^6+x^5+x^2+x+1)$ and $(x^6+x^5+x^4+x+1)$.

We conclude our investigations with some remarks:

Consider again $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and assume that the characteristic p of $\mathbb{F}_q$ does not divide m. Let $f := x^m - 1$. If t is the number of different irreducible factors of f in $\mathbb{F}_q[x]$, we have to do 2^t divisions and multiplications by applying the representation of P_f in (3.6). Following (4.2), the number of recursion steps is equal to t. But in each of these steps the operation $\odot$ which contains the composition and a division of polynomials has to be performed. (If the division is left out in each step, it is easy to see that we finally obtain a representation of P_f as a quotient of products of q-polynomials. This representation coincides with (3.6).)

The algorithm to compute cyclotomic polynomials in [11] is very efficient since the recursion contains a composition of polynomials of the simple form x^k (see also Example (4.4)). As mentioned above, for π-polynomials the situation is more complex.

By (3.6) the π-polynomial $P(f; x)$ has degree $\Phi_q(f)$. Using (2.5) it is not difficult to show that this number is at least $(q-1)^m$. Therefore it would be of certain practical interest to have some knowledge about the number of non-zero coefficients of this polynomial. In our example the number of terms of P_{x^6-1} is comparable with the number of terms of Q_{63}. By the analogy of (3.5) and (3.6) this might also hold in general.

Acknowledgements. The results of this paper formed part of the author's diplom thesis. He would like to thank Prof. Dr. Beutelspacher for supervision as well as Prof. Dr. Jungnickel for many helpful discussions.

References

1. Agnew, G. B., Mullin, R. C., Vanstone, S. A.: Arithmetic operations in GF(2^n). Submitted to J. Cryptology
2. Beth, T.: On the arithmetics of Galoisfields and the like. Proc. AAECC-3 Lecture Notes in Computer Sciences, vol. 229, pp. 2–16. Berlin, Heidelberg, New York, Springer 1986
3. Carlitz, L.: Primitive roots in a finite field. Trans. Am. Math. Soc. **73**, 373–382. (1952)
4. Cohen, S. D.: Primitive elements and polynomials with arbitrary trace. Discrete Math. **83**, 1–7 (1990)
5. Davenport, H.: Bases for finite fields. J. London Math. Soc. **43**, 21–49 (1968)
6. Jacobson, N.: Basic Algebra I. 2nd ed., Freeman W. H., New York: 1985
7. Jungnickel, D., Vanstone, S. A.: On primitive polynomials over finite fields. J. Algebra **124**, 337–353 (1989)
8. Landau, E.: Vorlesungen über Zahlentheorie II. Leipzig: Hirzel 1927
9. Lenstra, H. W., Jr., Schoof, R. J.: Primitive normal bases for finite fields. Math. Comp. **48**, 217–231 (1987)
10. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge: Cambridge University Press 1986
11. Lüneburg, H.: Galoisfelder, Kreisteilungspolynome und Schieberegisterfolgen. Mannheim: Bibliographisches Institut 1979
12. Meyberg, K.: Algebra 1, 2. München: Hanser- Verlag 1980/1976
13. Mullin, R. C., Onyszchuk, I. M., Vanstone, S. A., Wilson, R. M.: Optimal normal bases in GF(p^n). Discrete Appl. Math. **22**, 149-161 (1988/89)
14. Ore, O.: On a special class of polynomials. Trans. Am. Math. Soc. **35**, 559–584 (1933); Errata ibid., **36**, 275 (1934)
15. Ore, O.: Contributions to the theory of finite fields. Trans. Am. Math. Soc. **36**, 243–274 (1934)