Fast arithmetic with general Gauß periods

Joachim von zur Gathen, Michael Nöcker

Faculty of Computer Science, Electrical Engineering, and Mathematics
University of Paderborn
33095 Paderborn, Germany

Abstract

We show how to apply fast arithmetic in conjunction with general Gauß periods in finite fields. This is an essential ingredient for some efficient exponentiation algorithms.

Key words: exponentiation, finite fields, normal basis, Gauß period, efficient arithmetic

1 Introduction

Exponentiation is an important task with several applications in computer algebra and cryptography. If the ground domain is a finite field of "small" characteristic, then normal bases are a well-known and useful tool for this purpose. The goal of this paper is a computational framework in which one can combine the use of these normal bases with fast polynomial arithmetic.

If q is a prime power and $\mathbb{F}_{q^n}$ an extension of $\mathbb{F}_q$, then an element $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if its conjugates $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ are linearly independent over $\mathbb{F}_q$. A qth power of an element represented in this basis is just a cyclic shift of coordinates, and a general exponentiation also requires fewer operations than in the usual polynomial representation given by an irreducible polynomial. This is one reason why normal elements are an attractive data structure. An apparent drawback is that multiplication in this data structure is generally based on linear algebra and hence seems quite expensive.

* Corresponding author.
Email address: gathen@upb.de (Joachim von zur Gathen).
URL: http://www-math.upb.de/~aggathen/ (Joachim von zur Gathen).

A construction of special normal elements is via Gauß periods. We have an integer k, a prime number r with $nk = r - 1$, a primitive rth root of unity ζ in some extension of $\mathbb{F}_q$, a subgroup $\mathcal{K} \subseteq \mathbb{Z}_r^\times$ with k elements, and the **Gauß period**

$$\alpha = \sum_{a \in \mathcal{K}} \zeta^a .$$

Then $\alpha \in \mathbb{F}_{q^n}$, and it is normal over $\mathbb{F}_q$ if and only if q mod r and $\mathcal{K}$ generate the group $\mathbb{Z}_r^\times$, that is, $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$ (see Ash *et al.* (1989); Wassermann (1993)).

Rather than cumbersome matrix multiplication, as used for general normal bases, one can use polynomial multiplication to multiply elements in such a special normal basis. One can plug in any multiplication routine, from classical via Karatsuba to asymptotically fast ones (FFT-based or Cantor's method). This results in a speedup by an order of magnitude and the fastest exponentiation algorithms in large finite fields of small characteristic known today, both in theory and in software practice.

The time taken by the multiplication algorithm grows with the parameter k, which is extraneous to the base problem of calculating in $\mathbb{F}_{q^n}$. It is desirable to choose k small, ideally $k = 1$ or $k = 2$. (Then α is called an optimal normal basis; see Mullin *et al.* (1989)). But that is not always possible.

The applicability of this method was broadened by a recent generalization of Gauß periods from prime numbers r to arbitrary integers r. Gauß—who had used his periods for the construction of the regular 17-gon—had already presaged this, in Article 356 of his *Disquisitiones Arithmeticae*, but never published the general method: *"These theorems retain the same or even greater elegance when they are extended to composite values of n. But these matters are on a higher level of investigation, and we will reserve their consideration for another occasion."* [Gauß' n is the r used above.]

The goal of this paper is to show that the use of (fast) polynomial arithmetic is also feasible with these general Gauß periods. We achieve this in three steps: first, when r is a prime power, then when r is arbitrary and the Gauß period is of a special form, called *decomposable*. Lastly, we show that for an arbitrary Gauß period, we can always find a decomposable one with the same parameters.

Table 7.1 at the end of the paper shows that for roughly 35% of the field extensions in our experiments, general Gauß periods reduce the minimal value of k as compared to prime Gauß periods. The progress of the present work is to extend the applicability of polynomial arithmetic from the prime case to the general situation.

2 Gauß periods

In an arbitrary normal basis, all known multiplication algorithms such as the Massey-Omura multiplier make use of linear algebra. Our goal is to replace matrix-based multiplication by faster algorithms for specific normal elements, namely Gauß periods. This has been achieved by Gao *et al.* (1995), Gao *et al.* (1998), and Gao *et al.* (2000) for prime Gauß periods over $\mathbb{F}_q$, and also by Blake *et al.* (1998) for the special case of optimal normal bases (corresponding to $k \in \{1, 2\}$) in $\mathbb{F}_{2^n}$. Our results generalize all these.

In this section, we present Gauß periods and some of their properties for further use. We use the following notation throughout this paper.

NOTATION 2.1. *k, n, q, and r are positive integers with q a prime power, $r \geq 2$, $\gcd(q, r) = 1$, and $\phi(r) = nk$, where ϕ denotes* Euler's totient function*, and ζ is a primitive rth root of unity in an extension field of $\mathbb{F}_q$. Furthermore, $\mathcal{K}$ is a subgroup of $\mathbb{Z}_r^\times$ of order k.*

We let

$$r = r_1 \cdots r_t \text{ with } r_i = p_i^{e_i} \text{ for } 1 \leq i \leq t \tag{2.2}$$

be the *prime power factorization* of r, where $p_1, \ldots, p_t$ are pairwise distinct primes and $e_1, \ldots, e_t \in \mathbb{N}_{\geq 1}$. We call $R_1 = \prod_{1 \leq i \leq t, e_i = 1} p_i$ the *squarefree part* of r and $R_2 = r/R_1$ the *non-squarefree part*. (This is not to be confused with another common designation, namely that of $p_1 \cdots p_t$ as the squarefree part.) We say that r is *squarefree* when $r = R_1$. Feisel *et al.* (1999) introduced the following Gauß periods.

DEFINITION 2.3. *In the above notation, let*

$$b(x) = x^{R_2} \cdot \prod_{\substack{1 \leq i \leq t \\ p_i \mid R_2}} \sum_{1 \leq s \leq e_i} x^{r/p_i^s} \in \mathbb{F}_q[x]. \tag{2.4}$$

The Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ *given by ζ is defined as*

$$\alpha = \sum_{a \in \mathcal{K}} b(\zeta^a).$$

It is easy to see that $\alpha \in \mathbb{F}_{q^n}$. When r is prime, a prime power, or squarefree, we call α a prime, prime power, or squarefree Gauß period, respectively. The definition of α simplifies in these cases:

$$\begin{aligned} r \text{ prime or squarefree} &\implies \alpha = \sum_{a \in \mathcal{K}} \zeta^a, \\ r = p^e \text{ a prime power} &\implies \alpha = \sum_{\substack{a \in \mathcal{K} \\ 0 \leq s < e}} \zeta^{ap^s}. \end{aligned}$$

EXAMPLE 2.5. Let $q = 2$.

(i) Let $r = 5$, $\zeta \in \mathbb{F}_{2^4}$ a primitive 5th root of unity, and let $\mathcal{K} = \{1\}$ be the uniquely determined subgroup of $\mathbb{Z}_5^\times$ of order $k = 1$. Then $\alpha = \zeta$ is a *prime Gauß period* of type $(4, \{1\})$ in $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$.

(ii) Let $r = 3^2$, ζ a primitive 9th root of unity, and $\mathcal{K} = \{1, 8\}$. Then $\alpha = \zeta^{1\cdot 1} + \zeta^{3\cdot 1} + \zeta^{1\cdot 8} + \zeta^{3\cdot 8} = \zeta + \zeta^3 + \zeta^8 + \zeta^6$ is a *prime power Gauß period* of type $(3, \{1, 8\})$ in $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$.

(iii) Let $r = 3^2 \cdot 5$, and ζ be a primitive 45th root of unity. There are three subgroups of order $k = 2$ of $\mathbb{Z}_{45}^\times$ which define three different Gauß periods in $\mathbb{F}_{2^{12}}$. The subgroup $\mathcal{K}_1 = \{1, 26\}$ determines $\alpha_1 = \zeta^{14} + \zeta^{24} + \zeta^4 + \zeta^{39}$ of type $(12, \{1, 26\})$, $\mathcal{K}_2 = \{1, 44\}$ generates $\alpha_2 = \zeta^{14} + \zeta^{24} + \zeta^{21} + \zeta^{31}$, and $\mathcal{K}_3 = \{1, 19\}$ defines $\alpha_3 = \zeta^{14} + \zeta^{24} + \zeta^6 + \zeta^{41}$. ◊

We denote by $\langle q, \mathcal{K}\rangle = \{q^h a \colon h \in \mathbb{Z}, a \in \mathcal{K}\}$ the subgroup of $\mathbb{Z}_r^\times$ that is jointly generated by (q mod r) and $\mathcal{K}$. Normality of Gauß periods can be characterized by this subgroup.

NORMAL GAUSS PERIOD THEOREM 2.6 (Feisel *et al.* 1999). *Let α be the Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$. Then α is normal in $\mathbb{F}_{q^n}$ if and only if $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$.*

EXAMPLE 2.5 CONTINUED. (i) Since $\langle 2, \{1\}\rangle = \{2, 4, 3, 1\} = \mathbb{Z}_5^\times$, the Gauß period of type $(4, \{1\})$ is normal in $\mathbb{F}_{16}$ over $\mathbb{F}_2$.

(ii) One can easily check that $\langle 2, \{1, 8\}\rangle = \mathbb{Z}_9^\times$. Hence, the Gauß period of type $(3, \{1, 8\})$ is normal in $\mathbb{F}_8$ over $\mathbb{F}_2$.

(iii) Only the two subgroups $\mathcal{K}_1 = \{1, 26\}$ and $\mathcal{K}_2 = \{1, 44\}$ generate normal Gauß periods in $\mathbb{F}_{2^{12}}$ over $\mathbb{F}_2$. For $\mathcal{K}_3 = \{1, 19\}$ we have $\langle 2, \{1, 19\}\rangle = \{1, 2, 4, 8, 16, 17, 19, 23, 31, 32, 34, 38\} \neq \mathbb{Z}_{45}^\times$. Thus, the Gauß period of type $(12, \{1, 19\})$ over $\mathbb{F}_2$ is not normal in $\mathbb{F}_{4096}$. ◊

Two Gauß periods of the same type but given by different primitive rth roots of unity are conjugate.

The following is the main result of this paper.

THEOREM 2.7. *Let α be a normal Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$, and $r = r_1 \cdots r_t$ the prime power factorization (2.2) of r with $\mathcal{K} \subseteq \mathbb{Z}_r^\times$. Then there exists a normal Gauß period with the same parameters so that two elements in $\mathbb{F}_{q^n}$ represented in this normal basis can be multiplied with*

$$O(r \cdot \prod_{1 \le i \le t} (\log r_i \cdot \operatorname{loglog} r_i)) \text{ or } O(nk \log(nk) \operatorname{loglog}(nk))$$

operations in $\mathbb{F}_q$.

The proof is given at the end of Section 6.

3 Towers of groups and fields

Let α be a normal Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$, and σ the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Wassermann (1993), Bemerkung 3.1.2, observed that for a prime Gauß period, $q \mapsto \sigma$ induces an isomorphism from $\mathbb{Z}_r^\times/\mathcal{K}$ to $\mathrm{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q)$. This is also true for general Gauß periods.

Let $r' \geq 2$ be a divisor of r,

$$\pi_{r'} : \mathbb{Z}_r^\times \to \mathbb{Z}_{r'}^\times \text{ with } \pi_{r'}(a) = (a \bmod r') \tag{3.1}$$

the *canonical projection* of $\mathbb{Z}_r^\times$ onto $\mathbb{Z}_{r'}^\times$, and $\pi_{r'}(\mathcal{K})$ the image of $\mathcal{K} \subseteq \mathbb{Z}_r^\times$ under this epimorphism. Thus $\pi_{r'}(\mathcal{K})$ is a subgroup of $\mathbb{Z}_{r'}^\times$. The order k' of $\pi_{r'}(\mathcal{K})$ divides both $k = \#\mathcal{K}$ and $\phi(r') = \#\mathbb{Z}_{r'}^\times$. The following lemma states that the canonical projection gives a normal Gauß period in a subfield of $\mathbb{F}_{q^n}$.

Lemma 3.2. *Let α be a normal Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ given by ζ, $r' \geq 2$ a divisor of r, $\pi_{r'}$ as in (3.1), $k' = \#\pi_{r'}(\mathcal{K})$, and $n' = \phi(r')/k'$. Then n' divides n, $\zeta^{r/r'}$ is a primitive r'th root of unity, and the Gauß period α' of type $(n', \pi_{r'}(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to $\zeta^{r/r'}$ is normal in $\mathbb{F}_{q^{n'}}$ over $\mathbb{F}_q$.*

Proof. The canonical projection $\pi_{r'}$ is surjective, and $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$, hence $\langle \pi_{r'}(q), \pi_{r'}(\mathcal{K})\rangle = \mathbb{Z}_{r'}^\times$. The square of group homomorphisms in Figure 3.1 commutes. The top and right hand maps are surjective, and hence also the bottom one. It follows that $n' = \#\mathbb{Z}_{r'}^\times/\pi_{r'}(\mathcal{K})$ divides $n = \#\mathbb{Z}_r^\times/\mathcal{K}$. The other claims are clear. □

$$\begin{array}{ccc} \langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times & \xrightarrow{\pi_{r'}} & \mathbb{Z}_{r'}^\times = \langle \pi_{r'}(q), \pi_{r'}(\mathcal{K})\rangle \\ \big| & & \big| \\ \mathbb{Z}_r^\times/\mathcal{K} & \xrightarrow{\bar{\pi}_{r'}} & \mathbb{Z}_{r'}^\times/\pi_{r'}(\mathcal{K}) \end{array}$$

Figure 3.1. Four projection homomorphisms.

The connection between the group $\mathbb{Z}_r^\times$ and the normal Gauß period in a subfield plays an important rôle in what follows. We illustrate this in the case of

prime power Gauß periods. Let r be a prime power p^e with $e \geq 2$, and let ζ be a primitive p^eth root of unity. We suppose that the subgroup $\mathcal{K}$ of $\mathbb{Z}_r^\times$ defines a normal Gauß period $\alpha = \sum_{a\in\mathcal{K}} \sum_{0\leq s<e} \zeta^{ap^s}$ of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ with respect to ζ. Then $\langle q, \mathcal{K}\rangle = \mathbb{Z}_{p^e}^\times$. For $0 < \ell < e$, the element $\zeta_\ell = \zeta^{p^{e-\ell}}$ is a primitive p^ℓth root of unity, and we set $n_\ell = \phi(p^\ell)/\#\pi_{p^\ell}(\mathcal{K})$. Then

$$\alpha_\ell = \sum_{a\in\pi_{p^\ell}(\mathcal{K})} \sum_{0\leq s<\ell} \zeta_\ell^{ap^s}$$

is the Gauß period of type $(n_\ell, \pi_{p^\ell}(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to ζ_ℓ by Lemma 3.2. Since $\langle q, \pi_{p^\ell}(\mathcal{K})\rangle = \mathbb{Z}_{p^\ell}^\times$, the Gauß period α_ℓ is normal in $\mathbb{F}_{q^{n_\ell}}$ over $\mathbb{F}_q$.

Example 2.5 continued. (ii) The canonical projection $\pi_3 \colon \mathbb{Z}_9^\times \to \mathbb{Z}_3^\times$ maps $\mathcal{K} = \{1, 8\}$ onto the subgroup $\pi_3(\mathcal{K}) = \{1, 2\}$ of $\mathbb{Z}_3^\times$, and $\zeta_1 = \zeta^{3^{2-1}} = \zeta^3$ is a primitive third root of unity. Lemma 3.2 says that $\alpha_1 = \sum_{a\in\pi_3(\mathcal{K})} \zeta_1^a = \zeta^3 + \zeta^6 = 1$ is a normal Gauß period of type $(1, \{1, 2\})$ over $\mathbb{F}_2$. In fact, we have $\langle 2, \{1, 2\}\rangle = \mathbb{Z}_3^\times$, and α_1 is indeed a normal prime Gauß period. $\Diamond$

3.1 Cyclotomic polynomials

Primitive roots of unity are related to a special class of polynomials: the *cyclotomic polynomials*; see Lidl & Niederreiter (1983), Section 2.4 for details. When q is a prime power, r a positive integer coprime to q, and ζ a primitive rth root of unity over $\mathbb{F}_q$, then

$$\Phi_r = \prod_{\substack{0<s<r \\ \gcd(s,r)=1}} (x - \zeta^s) \in \mathbb{F}_q[x]$$

is the *rth cyclotomic polynomial* over $\mathbb{F}_q$. Since the roots of Φ_r are all $\phi(r)$ distinct primitive rth roots of unity, the degree of Φ_r is $\phi(r)$, and $\zeta \in \mathbb{F}_{q^{\phi(r)}}$.

Over the field $\mathbb{Q}$ of rational numbers, the cyclotomic polynomial Φ_r is always irreducible. This is no longer true in the case of a finite field $\mathbb{F}_q$ with nonzero characteristic. But in this case the factorization pattern is well-known.

Fact 3.3 (Lidl & Niederreiter 1983, Theorem 2.47). *Let q be a prime power coprime to a positive integer r, and let $N = \mathrm{ord}_r(q)$ be the order of q in $\mathbb{Z}_r^\times$. Then the rth cyclotomic polynomial $\Phi_r \in \mathbb{F}_q[x]$ factors into $\phi(r)/N$ distinct monic irreducible polynomials of the same degree N.*

We denote the $d = \phi(r)/N$ irreducible factors by $\mu_1, \ldots, \mu_d \in \mathbb{F}_q[x]$. By the *Chinese Remainder Theorem* we have the isomorphism of $\mathbb{F}_q$-algebras

$$\begin{aligned}\chi' : \mathcal{R} = \mathbb{F}_q[x]/(\Phi_r) &\to \mathbb{F}_q[x]/(\mu_1) \times \cdots \times \mathbb{F}_q[x]/(\mu_d) \\ A &\mapsto (A \bmod \mu_1, \ldots, A \bmod \mu_d).\end{aligned} \tag{3.4}$$

Since $\Phi_r(\zeta) = 0$ for any primitive rth root of unity $\zeta \in \mathbb{F}_{q^{\phi(r)}}$, we know that the minimal polynomial μ_ζ of ζ in $\mathbb{F}_q[x]$ is one of the $\mu_1, \ldots, \mu_d$. Then

$$\varphi_\zeta \colon \mathbb{F}_q(\zeta) \to \mathbb{F}_q[x]/(\mu_\zeta) \text{ with } \varphi_\zeta\left(\sum_{0 \le i < N} A_i \zeta^i\right) = \sum_{0 \le i < N} A_i (x^i \bmod \mu_\zeta)$$

is the canonical isomorphism between the two images of $\mathbb{F}_{q^N}$. The field $\mathbb{F}_q(\alpha)$ is a subfield of $\mathbb{F}_q(\zeta)$. Thus, we know the image of α in $\mathbb{F}_q[x]/(\mu_\zeta)$. The key for fast multiplication of Gauß periods lies in the choice of a suitable preimage of α in $\mathcal{R}$.

For any $i \le d$, let $c_i \in \mathcal{K}$ be such that $\zeta_i = \zeta^{c_i}$ is a root of μ_i. Then we have

$$\alpha = \sum_{a \in \mathcal{K}} b(\zeta^a) = \sum_{a \in \mathcal{K}} b(\zeta^{c_i a}) = \sum_{a \in \mathcal{K}} b({\zeta_i}^a),$$

since $a \mapsto ca$ is a bijection of $\mathcal{K}$. Applying the inverse isomorphism χ of χ', we have the preimage

$$\chi\left(\sum_{a \in \mathcal{K}} b(x^a \bmod \mu_1), \ldots, \sum_{a \in \mathcal{K}} b(x^a \bmod \mu_d)\right) = \sum_{a \in \mathcal{K}} b(x^a \bmod \Phi_r)$$

of α in $\mathcal{R}$. Finally, let $\varphi_{\zeta_1}, \ldots, \varphi_{\zeta_d}$ be the canonical isomorphisms with $\zeta_i = \zeta^{c_i}$ and $\mu_i(\zeta_i) = 0$ for $1 \le i \le d$. We define the homomorphism of $\mathbb{F}_q$-algebras

$$\begin{aligned}\varphi \colon \mathbb{F}_q(\alpha) &\to \mathcal{R} = \mathbb{F}_q[x]/(\Phi_r) \\ A &\mapsto \chi(\varphi_{\zeta_1}(A), \ldots, \varphi_{\zeta_d}(A)).\end{aligned} \tag{3.5}$$

If $A = \sum_{0 \le h < n} A_h \alpha^{q^h}$ is given as a linear combination of the conjugates of α, then

$$\varphi\Big(\sum_{0 \le h < n} A_h \alpha^{q^h}\Big) = \sum_{0 \le i < n} A_i \sum_{a \in \mathcal{K}} b(x^a \bmod \Phi_r).$$

This map allows us to transfer multiplication in the normal basis representation of $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ to multiplication in $\mathcal{R}$, which is just polynomial multiplication modulo Φ_r. Wonderful. The only drawback is that the original problem size is $n = \dim_{\mathbb{F}_q} \mathbb{F}_{q^n}$, while the new problem size $nk = \phi(r) = \dim_{\mathbb{F}_q} \mathcal{R}$ is larger by a factor of k. We want to keep this extraneous factor k as small as possible.

3.2 Field towers, traces, and normal elements

We conclude this section by collecting some well-known properties on normal elements that are useful subsequently. The properties listed below are true not only for normal Gauß periods but for all normal bases. We will discuss the algorithmic aspects for normal bases generated by Gauß periods in the subsequent sections.

3.2.1 The product of normal elements.

It is a well-known fact (see e.g. Menezes *et al.* (1993)) that normality is inherited along a *tower of fields*

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^{n_1}} \subseteq \mathbb{F}_{q^{n_1 n_2}} \subseteq \cdots \subseteq \mathbb{F}_{q^{n_1 \cdots n_t}},$$

whenever the degrees $n_1, \ldots, n_t \geq 1$ are pairwise coprime.

FACT 3.6. *Let n_1 and n_2 be two coprime positive integers, $n = n_1 \cdot n_2$, and α_i be a normal element in $\mathbb{F}_{q^{n_i}}$ over $\mathbb{F}_q$ for $i = 1, 2$. Then $\alpha = \alpha_1 \cdot \alpha_2$ is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Fact 3.6 shows a way to compute the multiplication matrix $T_{\mathcal{N}}$ of the normal basis $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n_1 n_2 - 1}})$ if $\gcd(n_1, n_2) = 1$ and the matrices $T_{\mathcal{N}_i}$ are already given for $i = 1, 2$.

FACT 3.7. *Let n_1, n_2 and α_1, α_2 as in Fact 3.6 and set $n = n_1 \cdot n_2$. Let $T_{\mathcal{N}_1} = (u_{j_1,h_1})_{0 \leq j_1,h_1 < n_1}$ and $T_{\mathcal{N}_2} = (v_{j_2,h_2})_{0 \leq j_2,h_2 < n_2}$ be the multiplication matrices of $\mathcal{N}_i = \{\alpha_i^{q^h} : 0 \leq h < n_i\}$ for $i = 1, 2$.*

(i) The multiplication matrix $T_{\mathcal{N}} = (t_{j,h})_{0 \leq j,h < n}$ of $\alpha = \alpha_1 \cdot \alpha_2$ is given by

$$t_{j,h} = u_{j_1,h_1} \cdot v_{j_2,h_2}$$

where $j \equiv j_i \bmod n_i$ and $h \equiv h_i \bmod n_i$ for $i = 1, 2$.

(ii) The density $d_{\mathcal{N}}$ of $T_{\mathcal{N}}$ is the product of the densities $d_{\mathcal{N}_1}$ and $d_{\mathcal{N}_2}$ of $T_{\mathcal{N}_1}$ and $T_{\mathcal{N}_2}$, respectively.

(iii) The multiplication matrix $T_{\mathcal{N}}$ can be calculated with $d_{\mathcal{N}} = d_{\mathcal{N}_1} \cdot d_{\mathcal{N}_2}$ multiplications in $\mathbb{F}_q$ from $T_{\mathcal{N}_1}$ and $T_{\mathcal{N}_2}$.

3.2.2 The trace of a normal element.

The trace also inherits normality. The next fact is true for all Galois extensions over a finite field, see Hachenberger (1997), Lemma 5.3. Thus the trace

map inherits normality downwards a field tower, while multiplication induces normality upwards.

FACT 3.8. *Let n_1 and n_2 be two coprime positive integers and $n = n_1 \cdot n_2$. If α is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then $\mathrm{Tr}_{q^n/q^{n_1}}(\alpha)$ is normal in $\mathbb{F}_{q^{n_1}}$ over $\mathbb{F}_q$.*

In the special case where $n = n_1 \cdot n_2$ is the product of two coprime factors we get some further useful properties. A proof of Lemma 3.9(i) is given in Jungnickel (1993), Lemma 5.1.8, and a special version of Lemma 3.9(ii) is cited in Agnew *et al.* (1993) for optimal normal bases. The proof technique will be used extensively in our algorithms, in particular analogs of the index maps Ψ_{n_1} and Ψ_{n_2}.

LEMMA 3.9. *Let n_1 and n_2 be coprime positive integers, $n = n_1 \cdot n_2$, and let α_1 and α_2 be normal in $\mathbb{F}_{q^{n_1}}$ and $\mathbb{F}_{q^{n_2}}$ over $\mathbb{F}_q$, respectively. Then*

(i) $\mathrm{Tr}_{q^n/q^{n_2}}(\alpha_1 \cdot \alpha_2) = \mathrm{Tr}_{q^{n_1}/q}(\alpha_1) \cdot \alpha_2$ *and*
(ii) α_2 *is normal in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_{q^{n_1}}$.

PROOF. (i) We have

$$\begin{aligned}\mathrm{Tr}_{q^n/q^{n_2}}(\alpha_1 \cdot \alpha_2) &= \sum_{0 \le i < n/n_2} (\alpha_1 \cdot \alpha_2)^{q^{in_2}} \\ &= \sum_{0 \le i < n/n_2} \alpha_1^{q^{in_2}} \cdot \alpha_2^{q^{in_2}} = \alpha_2 \cdot \sum_{0 \le i < n/n_2} \alpha_1^{q^{in_2}}\end{aligned}$$

since $\alpha_2 \in \mathbb{F}_{q^{n_2}}$, that is, $\alpha_2^{q^{in_2}} = \alpha_2$ for all $1 \le i < \frac{n}{n_2}$. Moreover, the map $\psi_{n_2} : \{0, \ldots, n_1 - 1\} \to \{0, \ldots, n_1 - 1\}$ with $\psi_{n_2}(i) = n_2 i \operatorname{rem} n_1$ is a bijection and hence

$$\sum_{0 \le i < n/n_2} \alpha_1^{q^{in_2}} = \sum_{0 \le i < n_1} \alpha_1^{q^i} = \mathrm{Tr}_{q^{n_1}/q}(\alpha_1).$$

(ii) Since $\mathcal{N}_2 = (\alpha_2, \ldots, \alpha_2^{q^{n_2-1}})$ is a basis for $\mathbb{F}_{q^{n_2}}$ over $\mathbb{F}_q$, the set $\mathcal{N}_2$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^{n_1}}$. By assumption, n_1 and n_2 are coprime, and hence the map $\psi_{n_1} : \{0, \ldots, n_2 - 1\} \to \{0, \ldots, n_2 - 1\}$ with $\psi_{n_1}(i) = n_1 i \operatorname{rem} n_2$ is a bijection. Therefore, the set $\{\alpha_2^{q^{n_1 h}} : 0 \le h < n_2\} = \{\alpha_2^{q^h} : 0 \le h < n_2\}$ is the set of all n_2 conjugates of α_2 over $\mathbb{F}_{q^{n_1}}$, and $\mathcal{N}_2$ is a normal basis over $\mathbb{F}_{q^{n_1}}$ as claimed. □

4 The prime power case

We are now ready to develop an algorithm that integrates polynomial multiplication in a normal basis representation whenever the normal element is a Gauß

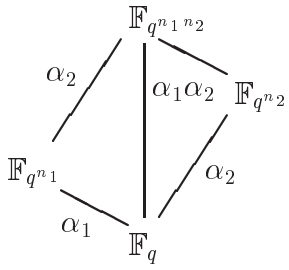

Figure 3.2. A tower of fields given by normal elements if $\gcd(n_1, n_2) = 1$.

period. In this section, we restrict to the case where $\alpha = \sum_{a\in\mathcal{K}} \sum_{0\le s<e} \zeta^{ap^s}$ is a prime or prime power Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$, that is, $r = p^e$. The main result of this section generalizes the approach that was described in Gao *et al.* (1995) and Gao *et al.* (2000) for prime Gauß periods.

Result 4.1. *Let p be a prime, e be a positive integer, and α be a normal prime power Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$, where $\mathcal{K}$ is a subgroup of $\mathbb{Z}_{p^e}^\times$. Two elements of $\mathbb{F}_{q^n}$ expressed in the normal basis $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n-1}})$ can be multiplied with at most $O(p^e \log p^e \cdot \operatorname{loglog} p^e)$ operations in $\mathbb{F}_q$.*

The underlying algorithm is one of the cornerstones of this paper. The algorithm consists of three parts: multiplication in $\mathbb{F}_q[x]/(x^{p^e} - 1)$, sorting the product to identify prime (power) Gauß periods in subfields of $\mathbb{F}_{q^n}$, and then applying the trace map to return to the linear combination of the conjugates of the prime (power) Gauß period.

4.1 An algorithm for fast multiplication

We start with an example illustrating the algorithmic ideas.

Example 4.2. Let ζ be a primitive 9th root of unity, and let α be the normal Gauß period of type $(3, \{1, 8\})$ over $\mathbb{F}_2$ as in Example 2.5(ii). The conjugates of $\alpha = \zeta + \zeta^3 + \zeta^8 + \zeta^6$ are $\alpha^{2^1} = \zeta^2 + \zeta^6 + \zeta^7 + \zeta^3$ and $\alpha^{2^2} = \zeta^4 + \zeta^3 + \zeta^5 + \zeta^6$.

(i) To calculate the product $\alpha^{2^2} \cdot \alpha$ as linear combination of $\alpha, \alpha^2, \alpha^4$, we regard the conjugates of α as elements of $\mathbb{F}_2(\zeta)$. The product in this extension field is

$$\alpha^4 \cdot \alpha = (\zeta^4 + \zeta^3 + \zeta^5 + \zeta^6) \cdot (\zeta + \zeta^3 + \zeta^8 + \zeta^6) = \zeta + \zeta^8$$

Both ζ and ζ^8 are summands of α. We complete the missing terms to get

$$\alpha^4 \cdot \alpha = (\zeta + \zeta^3 + \zeta^8 + \zeta^6) + \zeta^3 + \zeta^6.$$

(ii) Observe that ζ^3 and ζ^6 are primitive third roots of unity over $\mathbb{F}_2$. We apply the canonical projection $\pi_3\colon \mathbb{Z}_9^\times \to \mathbb{Z}_3^\times$ as defined in (3.1). Then $\pi_3(\{1,8\}) = \{1,2\} = \mathbb{Z}_3^\times$ and hence $n' = \phi(3)/\#\{1,2\} = 1$. Thus, the projection generates the prime Gauß period $\alpha_1 = \zeta^3 + (\zeta^3)^2$ over $\mathbb{F}_2$. We substitute $\zeta^3 + \zeta^6$ by α_1 to get

$$\alpha^4 \cdot \alpha = \alpha + \alpha_1.$$

(iii) In order to express α_1 as a linear combination of the conjugates of α we compute the trace of α over $\mathbb{F}_2$:

$$\begin{aligned}\mathrm{Tr}_{2^3/2^1}(\alpha) &= \sum_{0\le i<3} \alpha^{2^i} = \alpha + \alpha^2 + \alpha^4 \\ &= (\zeta + \zeta^3 + \zeta^8 + \zeta^6) + (\zeta^2 + \zeta^6 + \zeta^7 + \zeta^3) + (\zeta^4 + \zeta^3 + \zeta^5 + \zeta^6) \\ &= \zeta + \zeta^7 + \zeta^4 + \zeta^8 + \zeta^2 + \zeta^5 + \zeta^3 + \zeta^6.\end{aligned}$$

We sort the summands and apply the fact that $0 = \Phi_3(\zeta^3) = 1 + \zeta^3 + \zeta^6$ to get

$$\begin{aligned}\mathrm{Tr}_{2^3/2^1}(\alpha) &= \zeta \cdot (1 + \zeta^6 + \zeta^3) + \zeta^2 \cdot (\zeta^6 + 1 + \zeta^3) + \zeta^3 + \zeta^6 \\ &= \zeta^3 + \zeta^6 = \alpha_1.\end{aligned}$$

Indeed, the trace describes a linear combination of the conjugates of α for α_1. We insert this linear combination

$$\alpha^4 \cdot \alpha = \alpha + \alpha_1 = \alpha + \mathrm{Tr}_{2^3/2^1}(\alpha) = \alpha^2 + \alpha^4$$

which completes the computation. ◊

We will show that the map $\varphi\colon \mathbb{F}_q(\alpha) \to \mathcal{R} = \mathbb{F}_q[x]/(\Phi_{p^e})$ as in 3.5 is in fact an injective ring homomorphism if α is normal over $\mathbb{F}_q$.

4.1.1 A sum of Gauß periods.

We use the following notation.

NOTATION 4.3. *Let ζ be a primitive p^eth root of unity. For $0 < \ell \le e$ let π_{p^ℓ} be the canonical projection from $\mathbb{Z}_{p^e}^\times$ onto $\mathbb{Z}_{p^\ell}^\times$. Set $k_\ell = \#\pi_{p^\ell}(\mathcal{K})$ and $n_\ell = \phi(p^\ell)/k_\ell$. The Gauß period of type $(n_\ell, \pi_{p^\ell}(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to $\zeta_\ell = \zeta^{p^{e-\ell}}$ is denoted by α_ℓ. We set $n_0 = k_0 = 1$.*

We take a look at the summands of the product $\varphi(A) \cdot \varphi(B)$, and want to write a preimage of φ of this product in $\mathbb{F}_q[x]/(x^{p^e} - 1)$ in a particular way. We note that $x^a \equiv x^b \bmod (x^{p^e} - 1)$ if $a \equiv b \bmod p^e$.

For all $0 \leq i < n$, we define the positive integers

$$\begin{aligned} u_{\ell,h}^{(i)} &= \#\{a \in \mathcal{K} \colon 1 + aq^i \in p^{e-\ell} q^h \mathcal{K}\} \text{ for } 0 < \ell \leq e \text{ and } 0 \leq h < n_\ell, \\ v_{\ell,h}^{(i)} &= \#\{a \in \mathcal{K} \colon 1 + ap^\ell q^i \in q^h \mathcal{K}\} \quad \text{for } 0 < \ell < e \text{ and } 0 \leq h < n_\ell. \end{aligned} \tag{4.4}$$

Furthermore, we set

$$u_{0,0}^{(i)} = \begin{cases} 1 \text{ if there is } a \in q^i\mathcal{K} \text{ such that } 1 + aq^i \equiv 0 \bmod p^e, \text{ and} \\ 0 \text{ otherwise.} \end{cases}$$

These numbers define the *special form* of the preimage in $\mathbb{F}_q[x]/(x^{p^e} - 1)$ of $\varphi(A) \cdot \varphi(B)$ that we are looking for. Subsequently, we suppose that $\langle q, \mathcal{K} \rangle = \mathbb{Z}_{p^e}^\times$. Since φ is additive, it is sufficient to look at the following product. A generalization is shown in Proposition 4.10.

Lemma 4.5. *Let $0 \leq i < n$ and $\mathbb{F}$ be the prime subfield of $\mathbb{F}_q$. Then there are $C_0^{(i)}$ and $C_{\ell,h}^{(i)}$ in $\mathbb{F}$ for $0 < \ell \leq e$ and $0 \leq h < n_\ell$ such that*

$$\begin{aligned} &\left(\sum_{a \in \mathcal{K}} \sum_{0 \leq s < e} x^{ap^s q^i} \right) \cdot \left(\sum_{b \in \mathcal{K}} \sum_{0 \leq s' < e} x^{bp^{s'}} \right) \\ &\equiv C_0^{(i)} + \sum_{0 < \ell \leq e} \sum_{0 \leq h < n_\ell} C_{\ell,h}^{(i)} \left(\sum_{a \in \pi_{p^\ell}(\mathcal{K})} \sum_{0 \leq s < \ell} (x^{p^{e-\ell}})^{ap^s} \right)^{q^h} \bmod (x^{p^e} - 1). \end{aligned}$$

Since ζ is a root of $(x^{p^e} - 1)$, the product of α^{q^i} times α can be written as a sum of those Gauß periods α_ℓ which are given by the canonical projection of $\mathcal{K}$ onto $\mathbb{Z}_{p^\ell}^\times$.

Corollary 4.6. *Let α be the Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ with respect to ζ. For $0 < \ell \leq e$, let α_ℓ be the Gauß period of type $(n_\ell, \pi_{p^\ell}(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to $\zeta^{p^{e-\ell}}$. For $0 \leq i < n$, let $C_0^{(i)}$ and $C_{\ell,h}^{(i)}$ for $0 \leq \ell < e$ and $0 \leq h < n_\ell$ as in Lemma 4.5. Then*

$$\alpha^{q^i} \cdot \alpha = C_0^{(i)} + \sum_{0 < \ell \leq e} \sum_{0 \leq h < n_\ell} C_{\ell,h}^{(i)} \alpha_\ell^{q^h}.$$

We start with a proposition that describes the coefficients of the preimage of $\varphi(A) \cdot \varphi(B)$ in $\mathbb{F}_q[x]/(x^{p^e} - 1)$ in terms of $u_{\ell,h}^{(i)}$ and $v_{\ell,h}^{(i)}$.

PROPOSITION 4.7. *Let $0 \le i < n$ be fixed and $u_{\ell,h}^{(i)}$ and $v_{\ell,h}^{(i)}$ as in (4.4). Set*

$$\begin{aligned} C'_0 &= k \cdot \textstyle\sum_{0\le\ell\le e} \Big((e-\ell)\cdot \sum_{0\le h<n_\ell} u_{\ell,h}^{(i)}\Big) \qquad \text{and} \\ C'_{p^{e-\ell}q^h} &= \tfrac{k}{k_\ell}\cdot\Big(\textstyle\sum_{\ell\le s\le e} u_{s,h}^{(i)} + \sum_{0<s<\ell}(v_{s,h}^{(i)} + v_{s,h-i}^{(n-i)})\Big) \\ &\qquad \text{for all } 0<\ell\le e \text{ and } 0\le h<n_\ell. \end{aligned}$$

Then

$$\begin{aligned} &\Bigg(\sum_{a\in\mathcal{K}}\sum_{0\le s<e} x^{ap^sq^i}\Bigg)\cdot\Bigg(\sum_{b\in\mathcal{K}}\sum_{0\le s'<e} x^{bp^{s'}}\Bigg) \\ &\equiv C'_0 + \sum_{0<\ell\le e}\sum_{0\le h<n_\ell} C'_{p^{e-\ell}q^h} \sum_{a\in\pi_{p^\ell}(\mathcal{K})} (x^{p^{e-\ell}})^{aq^h} \bmod (x^{p^e}-1). \end{aligned}$$

PROOF. A straightforward computation gives

$$\begin{aligned} &\Bigg(\sum_{\substack{a\in\mathcal{K}\\0\le s<e}} x^{ap^sq^i}\Bigg)\cdot\Bigg(\sum_{\substack{b\in\mathcal{K}\\0\le s'<e}} x^{bp^{s'}}\Bigg) = \sum_{\substack{a,b\in\mathcal{K}\\0\le s,s'<e}} x^{ap^sq^i+bp^{s'}} \\ &= \sum_{a,b\in\mathcal{K}}\Bigg(\sum_{0\le s<e} x^{ap^sq^i+bp^{s+0}} + \sum_{\substack{0<\ell<e\\0\le s<e-\ell}} (x^{ap^{s+\ell}q^i+bp^s} + x^{ap^sq^i+bp^{s+\ell}})\Bigg) \\ &\equiv \sum_{\substack{a,b\in\mathcal{K}\\0\le s<e}} x^{bp^s(1+aq^i)} + \sum_{\substack{a,b\in\mathcal{K}\\0<\ell<e\\0\le s<e-\ell}} x^{bp^s(1+ap^\ell q^i)} \\ &\quad + \sum_{\substack{a,b\in\mathcal{K}\\0<\ell<e\\0\le s<e-\ell}} x^{ap^sq^i(1+bp^\ell q^{n-i})} \bmod (x^{p^e}-1). \end{aligned}$$

We consider the three major summands separately.

Fix $a \in \mathcal{K}$. Then $1+aq^i$ is either equal 0 modulo p^e or there are $0<\ell\le e$ and $0\le h<n_\ell$ such that $1+aq^i \in p^{e-\ell}q^h\mathcal{K} \subseteq \mathbb{Z}_{p^e}$. Then

$$\sum_{\substack{b\in\mathcal{K}\\0\le s<e}} x^{bp^s(1+aq^i)} \equiv \sum_{\substack{b\in\mathcal{K}\\0\le s<e}} x^0 \equiv ke \bmod (x^{p^e}-1)$$

if $1+aq^i \equiv 0 \bmod p^e$, and otherwise we have

$$\begin{aligned}\sum_{\substack{b\in\mathcal{K}\\0\le s<e}} x^{bp^s(1+aq^i)} &\equiv \sum_{\substack{b\in\mathcal{K}\\0\le s<e}} x^{bp^s p^{e-\ell}q^h} \equiv \sum_{b\in\mathcal{K}}\left(\sum_{0\le s<\ell} x^{bp^{e-(\ell-s)}q^h} + \sum_{\ell\le s<e} x^{bp^{e+(s-\ell)}q^h}\right)\\ &\equiv \sum_{\substack{b\in\mathcal{K}\\0\le s<\ell}} x^{bp^{e-(\ell-s)}q^h} + \sum_{b\in\mathcal{K}}(e-\ell)\\ &\equiv \sum_{0<s\le\ell}\frac{k}{k_s}\sum_{b\in\pi_{p^s}(\mathcal{K})}(x^{p^{e-s}})^{bq^h} + k(e-\ell) \bmod (x^{p^e}-1).\end{aligned}$$

If a runs through $\mathcal{K}$ then we get the first intermediate result as

$$\begin{aligned}&\sum_{a\in\mathcal{K}}\left(\sum_{\substack{b\in\mathcal{K}\\0\le s<e}} x^{bp^s(1+aq^i)}\right)\\ &\equiv \sum_{\substack{0<\ell\le e\\0\le h<n_\ell}} u^{(i)}_{\ell,h}\cdot\left(\sum_{0<s\le\ell}\frac{k}{k_s}\sum_{b\in\pi_{p^s}(\mathcal{K})}(x^{p^{e-s}})^{bq^h} + k(e-\ell)\right) + u^{(i)}_{0,0}ke\\ &\equiv k\cdot\sum_{0\le\ell<e}\left((e-\ell)\cdot\sum_{0\le h<n_\ell}u^{(i)}_{\ell,h}\right)\\ &\quad+\sum_{\substack{0<\ell\le e\\0\le h<n_\ell}}\left(\frac{k}{k_\ell}\sum_{\ell\le s\le e}u^{(i)}_{s,h}\right)\left(\sum_{b\in\pi_{p^\ell}(\mathcal{K})}(x^{p^{e-\ell}})^b\right)^{q^h} \bmod (x^{p^e}-1).\end{aligned}$$

For the second sum, we fix $a\in\mathcal{K}$ and $0<\ell<e$. Since $1+ap^\ell q^h\in\mathbb{Z}_{p^e}^\times$ and $\langle q,\mathcal{K}\rangle=\mathbb{Z}_{p^e}^\times$, there is $0\le h<n$ such that $1+ap^\ell q^i\in q^h\mathcal{K}$. Then we get

$$\begin{aligned}\sum_{\substack{b\in\mathcal{K}\\0\le s<e-\ell}} x^{bp^s(1+ap^\ell q^i)} &\equiv \sum_{\substack{b\in\mathcal{K}\\0\le s<e-\ell}} x^{bp^s q^h}\\ \equiv \sum_{\substack{b\in\mathcal{K}\\\ell<s\le e}}(x^{p^{e-s}})^{bq^h} &\equiv \sum_{\ell<s\le e}\frac{k}{k_s}\sum_{b\in\pi_{p^s}(\mathcal{K})}(x^{p^{e-s}})^{bq^h} \bmod (x^{p^e}-1).\end{aligned}$$

If a runs through $\mathcal{K}$ then the sum over all $0<\ell<e$ is given by

$$\begin{aligned}&\sum_{\substack{a\in\mathcal{K}\\0<\ell<e}}\left(\sum_{\substack{b\in\mathcal{K}\\0\le s<e-\ell}} x^{bp^s(1+ap^\ell q^i)}\right)\\ &\equiv \sum_{\substack{0<\ell<e\\0\le h<n_\ell}} v^{(i)}_{\ell,h}\cdot\left(\sum_{\ell<s\le e}\frac{k}{k_s}\cdot\sum_{b\in\pi_{p^s}(\mathcal{K})}(x^{p^{e-s}})^{bq^h}\right)\\ &\equiv \sum_{\substack{1<\ell\le e\\0\le h<n_\ell}}\left(\frac{k}{k_\ell}\sum_{0<s<\ell}v^{(i)}_{s,h}\right)\left(\sum_{b\in\pi_{p^\ell}(\mathcal{K})}(x^{p^{e-\ell}})^b\right)^{q^h} \bmod (x^{p^e}-1).\end{aligned}$$

By changing the rôles of a and b and substituting i by $n-i$, we get the formula

for the third summand:

$$\begin{aligned}
&\sum_{\substack{b\in\mathcal{K}\\0<\ell<e}}\Bigg(\sum_{\substack{a\in\mathcal{K}\\0\le s<e-\ell}} x^{ap^s(1+bp^\ell q^{n-i})}\Bigg)^{q^i}\\
&\equiv \sum_{\substack{1<\ell\le e\\0\le h<n_\ell}}\left(\frac{k}{k_\ell}\sum_{0<s<\ell} v_{s,h}^{(n-i)}\right)\Bigg(\sum_{a\in\pi_{p^\ell}(\mathcal{K})}(x^{p^{e-\ell}})^a\Bigg)^{q^{i+h}}\\
&\equiv \sum_{\substack{1<\ell\le e\\0\le h<n_\ell}}\left(\frac{k}{k_\ell}\sum_{0<s<\ell} v_{s,h-i}^{(n-i)}\right)\Bigg(\sum_{a\in\pi_{p^\ell}(\mathcal{K})}(x^{p^{e-\ell}})^a\Bigg)^{q^h} \bmod (x^{p^e}-1). \qquad \square
\end{aligned}$$

With the help of this proposition, we can group all summands of the preimage of $\varphi(A)\cdot\varphi(B)$ in $\mathbb{F}_q[x]/(x^{p^e}-1)$—except the constant coefficient—in terms of $\sum_{a\in\pi_{p^\ell}(\mathcal{K})}(x^{p^{e-\ell}})^{aq^h}$ with $0<\ell\le e$ and $0\le h<n_\ell$. Let $0\le i<n$ be fixed as before; we omit it in the notation. Now our approach is to sort these terms into sums which are preimages of α_ℓ, for $0<\ell\le e$, in $\mathcal{R}$. This is obvious but a little bit technical. Thus, we want to define two useful sequences of integers for all $0<\ell\le e$, $\ell\le s<e$, and $0\le h<n_\ell$:

$$\begin{aligned}
D_{\ell,h}^{(e)} &= 0,\\
C_{\ell,h} &= C'_{p^{e-\ell}q^h} - D_{\ell,h}^{(\ell)},\\
D_{\ell,h}^{(s)} &= D_{\ell,h}^{(s+1)} + \tfrac{k_{s+1}}{k_\ell}\textstyle\sum_{0\le j<\frac{n_{s+1}}{n_\ell}} C_{s+1,h+jn_\ell}.
\end{aligned} \tag{4.8}$$

Informally speaking, the $D_{\ell,h}^{(s)}$ are those parts of the $C'_{p^{e-\ell}q^h}$ which have already been identified as Gauß periods. We give some alternative computations of the $D_{\ell,h}^{(s)}$ to illustrate this.

LEMMA 4.9. *Let $D_{\ell,h}^{(s)}$ and $C_{\ell,h}$ be as above. Then*

(i) $D_{\ell,h}^{(s)} = \sum_{s\le s'<e}\frac{k_{s'+1}}{k_\ell}\left(\sum_{0\le j<\frac{n_{s'+1}}{n_\ell}} C_{s'+1,h+jn_\ell}\right)$ *for* $0<\ell\le s<e$,

(ii) $D_{\ell,h}^{(\ell+1)} = \frac{k_{\ell+1}}{k_\ell}\sum_{0\le j<\frac{n_{\ell+1}}{n_\ell}} D_{\ell+1,h+jn_\ell}^{(\ell+1)}$ *for* $0<\ell<e$,

(iii) $D_{\ell,h}^{(\ell)} = \frac{k_{\ell+1}}{k_\ell}\sum_{0\le j<\frac{n_{\ell+1}}{n_\ell}}\left(D_{\ell+1,h+jn_\ell}^{(\ell+1)} + C_{\ell+1,h+jn_\ell}\right)$ *for* $0<\ell<e$.

PROOF. (i) We proceed by induction on s. For $s=e-1$, by definition we

have for all $0 < \ell < e$ that

$$D_{\ell,h}^{(e-1)} = D_{\ell,h}^{(e)} + \frac{k_e}{k_\ell} \sum_{0 \le j < \frac{n_e}{n_\ell}} C_{e,h+jn_\ell}$$
$$= \sum_{e-1 \le s' < e} \frac{k_{s'+1}}{k_\ell} \Bigg(\sum_{0 \le j < \frac{n_{s'+1}}{n_\ell}} C_{s'+1,h+jn_\ell} \Bigg),$$

using $D_{\ell,h}^{(e)} = 0$. We suppose that the claimed formula is also true for $1 < s+1 < e$. Inserting the induction hypothesis into the definition of $D_{\ell,h}^{(s)}$ gives

$$D_{\ell,h}^{(s)} = D_{\ell,h}^{(s+1)} + \frac{k_{s+1}}{k_\ell} \Bigg(\sum_{0 \le j < \frac{n_{s+1}}{n_\ell}} C_{s+1,h+jn_\ell} \Bigg)$$
$$= \sum_{s+1 \le s' < e} \frac{k_{s'+1}}{k_\ell} \Bigg(\sum_{0 \le j < \frac{n_{s'+1}}{n_\ell}} C_{s'+1,h+jn_\ell} \Bigg) + \frac{k_{s+1}}{k_\ell} \sum_{0 \le j < \frac{n_{s+1}}{n_\ell}} C_{s+1,h+jn_\ell}$$
$$= \sum_{s \le s' < e} \frac{k_{s'+1}}{k_\ell} \Bigg(\sum_{0 \le j < \frac{n_{s'+1}}{n_\ell}} C_{s'+1,h+jn_\ell} \Bigg),$$

and the induction step is complete.

(ii) Let $0 < \ell < e$. Then

$$D_{\ell,h}^{(\ell+1)} = \sum_{\ell+1 \le s' < e} \frac{k_{s'+1}}{k_\ell} \Bigg(\sum_{0 \le j < \frac{n_{s'+1}}{n_\ell}} C_{s'+1,h+jn_\ell} \Bigg)$$

by (i). We sort the summands and use (i) again to obtain

$$D_{\ell,h}^{(\ell+1)} = \sum_{\ell+1 \le s' < e} \frac{k_{\ell+1}}{k_\ell} \cdot \frac{k_{s'+1}}{k_{\ell+1}} \Bigg(\sum_{0 \le j < \frac{n_{\ell+1}}{n_\ell}} \sum_{0 \le i < \frac{n_{s'+1}}{n_{\ell+1}}} C_{s'+1,h+(jn_\ell + in_{\ell+1})} \Bigg)$$

$$= \frac{k_{\ell+1}}{k_\ell} \cdot \sum_{0 \le j < \frac{n_{\ell+1}}{n_\ell}} \Bigg(\sum_{\ell+1 \le s' < e} \frac{k_{s'+1}}{k_{\ell+1}} \Bigg(\sum_{0 \le i < \frac{n_{s'+1}}{n_{\ell+1}}} C_{s'+1,(h+jn_\ell)+in_{\ell+1}} \Bigg) \Bigg)$$
$$= \frac{k_{\ell+1}}{k_\ell} \cdot \sum_{0 \le j < \frac{n_{\ell+1}}{n_\ell}} D_{\ell+1,h+jn_\ell}^{(\ell+1)}.$$

(iii) We use induction on ℓ. For $\ell = e-1$, we have by definition

$$D_{e-1,h}^{(e-1)} = D_{e-1,h}^{(e)} + \frac{k_e}{k_{e-1}} \sum_{0 \le j < \frac{n_e}{n_{e-1}}} C_{e,h+jn_{e-1}},$$

which is just the claimed formula since $D_{\ell,h}^{(e)} = 0$ for all $0 < \ell \leq e$. We assume that the claim also holds for $1 < \ell + 1 < e$. Then (ii) gives

$$\begin{aligned} D_{\ell,h}^{(\ell)} &= D_{\ell,h}^{(\ell+1)} + \frac{k_{\ell+1}}{k_\ell} \sum_{0 \leq j < \frac{n_{\ell+1}}{n_\ell}} C_{\ell+1,h+jn_\ell} \\ &= \frac{k_{\ell+1}}{k_\ell} \sum_{0 \leq j < \frac{n_{\ell+1}}{n_\ell}} \left(D_{\ell+1,h+jn_\ell}^{(\ell+1)} + C_{\ell+1,h+jn_\ell} \right). \end{aligned}$$

□

We prove with the help of these sequences $D_{\ell,h}^{(s)}$ and $C_{\ell,h}$ that the preimage of $\varphi(A) \cdot \varphi(B)$ in $\mathbb{F}_q[x]/(x^{p^e} - 1)$ can be written as a sum of Gauß periods. The following proposition includes Lemma 4.5 as the special case $\ell' = 0$.

PROPOSITION 4.10. *Let $C_{\ell,h}$ and $D_{\ell,h}^{(s)}$ be as in (4.8), and $0 \leq \ell' \leq e$. Then*

$$\begin{aligned} &\left(\sum_{\substack{a \in \mathcal{K} \\ 0 \leq s < e}} x^{ap^s q^i} \right) \cdot \left(\sum_{\substack{b \in \mathcal{K} \\ 0 \leq s' < e}} x^{bp^{s'}} \right) \\ &\equiv C'_0 \sum_{\substack{\ell' < \ell \leq e \\ 0 \leq h < n_\ell}} C_{\ell,h} \cdot \left(\sum_{a \in \pi_{p^\ell}(\mathcal{K})} \sum_{0 \leq s < \ell} (x^{p^{e-\ell}})^{ap^s} \right)^{q^h} \\ &\quad + \sum_{\substack{0 < \ell \leq \ell' \\ 0 \leq h < n_\ell}} \left(C'_{p^{e-\ell} q^h} - D_{\ell,h}^{(\ell')} \right) \cdot \left(\sum_{a \in \pi_{p^\ell}(\mathcal{K})} x^{p^{e-\ell} a q^h} \right) \bmod (x^{p^e} - 1) \end{aligned}$$

for all $0 \leq \ell' \leq e$.

PROOF. We use induction on ℓ'. For $\ell' = e$, the right hand side of the claimed equation is

$$C'_0 + 0 + \sum_{\substack{0 < \ell \leq e \\ 0 \leq h < n_\ell}} \left(C'_{p^{e-\ell} q^h} - D_{\ell,h}^{(e)} \right) \cdot \left(\sum_{a \in \pi_{p^\ell}(\mathcal{K})} x^{p^{e-\ell} a q^h} \right)$$

which is just the right hand side of the congruence in Proposition 4.7, since all $D_{\ell,h}^{(e)}$ are zero. Now, we suppose that the formula is true for an $\ell \in \mathbb{N}_{>0}$ with $0 < \ell' \leq \ell \leq e$. Then for all $0 \leq h < n_{\ell'}$

$$
\begin{aligned}
&\left(C'_{p^{e-\ell'}q^h} - D^{(\ell')}_{\ell',h}\right) \cdot \left(\sum_{a\in\pi_{p^{\ell'}}(\mathcal{K})} x^{p^{e-\ell'}aq^h}\right)\\
&\overset{(4.8)}{\equiv} C_{\ell',h} \cdot \sum_{a\in\pi_{p^{\ell'}}(\mathcal{K})} \left(\sum_{0\le s<\ell'} x^{p^{e-\ell'}ap^sq^h} - \sum_{1\le s<\ell'} x^{p^{e-\ell'}ap^sq^h}\right)\\
&\equiv \left(C_{\ell',h} \cdot \sum_{a\in\pi_{p^{\ell'}}(\mathcal{K})} \sum_{0\le s<\ell'} x^{p^{e-\ell'}ap^sq^h}\right) - \left(C_{\ell',h} \cdot \sum_{a\in\pi_{p^{\ell'}}(\mathcal{K})} \sum_{1\le s<\ell'} x^{p^{e-(\ell'-s)}aq^h}\right)\\
&\quad \bmod (x^{p^e}-1).
\end{aligned}
$$

We sort the summands by adding the first term of the difference to the already collected summands

$$
\begin{aligned}
&C'_0 + \sum_{\ell'<\ell\le e} \sum_{0\le h<n_\ell} C_{\ell,h} \cdot \left(\sum_{a\in\pi_{p^\ell}(\mathcal{K})} \sum_{0\le s<\ell} (x^{p^{e-\ell}})^{ap^s}\right)^{q^h}\\
&+ \sum_{0\le h<n_{\ell'}} C_{\ell',h} \cdot \sum_{a\in\pi_{p^{\ell'}}(\mathcal{K})} \sum_{0\le s<\ell'} x^{p^{e-\ell'}ap^sq^h}\\
\equiv\, &C'_0 + \sum_{\ell'\le\ell\le e} \sum_{0\le h<n_\ell} C_{\ell,h} \cdot \left(\sum_{a\in\pi_{p^\ell}(\mathcal{K})} \sum_{0\le s<\ell} (x^{p^{e-\ell}})^{ap^s}\right)^{q^h} \bmod (x^{p^e}-1).
\end{aligned}
$$

The remaining part is

$$
\begin{aligned}
&\sum_{\substack{0<\ell<\ell'\\ 0\le h<n_\ell}} \left(C'_{p^{e-\ell}q^h} - D^{(\ell')}_{\ell,h}\right) \cdot \left(\sum_{a\in\pi_{p^\ell}(\mathcal{K})} x^{p^{e-\ell}aq^h}\right)\\
&- \sum_{0\le h<n_{\ell'}} C_{\ell',h} \cdot \sum_{a\in\pi_{p^{\ell'}}(\mathcal{K})} \sum_{1\le s<\ell'} x^{p^{e-(\ell'-s)}aq^h}\\
\equiv &\sum_{\substack{0<\ell<\ell'\\ 0\le h<n_\ell}} \left(C'_{p^{e-\ell}q^h} - D^{(\ell')}_{\ell,h}\right) \cdot \left(\sum_{a\in\pi_{p^\ell}(\mathcal{K})} x^{p^{e-\ell}aq^h}\right)\\
&- \sum_{0\le h<n_{\ell'}} C_{\ell',h} \cdot \sum_{1\le s<\ell'} \frac{k_{\ell'}}{k_s} \sum_{a\in\pi_{p^s}(\mathcal{K})} (x^{p^{e-s}})^{aq^h}\\
\equiv &\sum_{\substack{0<\ell<\ell'\\ 0\le h<n_\ell}} \left(C'_{p^{e-\ell}q^h} - \left(D^{(\ell')}_{\ell,h} + \frac{k_{\ell'}}{k_\ell} \cdot \sum_{0\le j<\frac{n_{\ell'}}{n_\ell}} C_{\ell',h+jn_\ell}\right)\right)\\
&\cdot \left(\sum_{a\in\pi_{p^\ell}(\mathcal{K})} x^{p^{e-\ell}aq^h}\right) \bmod (x^{p^e}-1).
\end{aligned}
$$

But $D^{(\ell')}_{\ell,h} + \frac{k_{\ell'}}{k_\ell} \sum_{0\le i<\frac{n_{\ell'}}{n_\ell}} C_{\ell',h+in_\ell} = D^{(\ell'-1)}_{\ell,h}$ by construction in (4.8), and the induction step follows. □

4.1.2 Applying the trace map.

The last ingredient is the trace map. It provides a way of writing a normal Gauß period $\alpha_\ell \in \mathbb{F}_{q^{n_\ell}}$ as a linear combination of the elements of the normal basis $\mathcal{N} = (\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ of $\mathbb{F}_{q^n}$.

LEMMA 4.11. *Let $r = p^e$ be a prime power, and let α be a prime power Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ with respect to ζ, where $\langle q, \mathcal{K}\rangle = \mathbb{Z}_{p^e}^\times$. For any $0 < \ell \le e$, let α_ℓ be the Gauß period of type $(n_\ell, \pi_{p^\ell}(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to $\zeta^{p^{e-\ell}}$. Then*

$$\sum_{0 \le i < \frac{n}{n_\ell}} \alpha^{q^{in_\ell}} = p^{e-\ell}\alpha_\ell \text{ for } 0 < \ell \le e.$$

Furthermore, we have

$$\sum_{0 \le i < n} \alpha^{q^i} = -p^{e-1}.$$

We again derive these formulas step by step, and will give a proof of Lemma 4.11 as a conclusion at the end of this paragraph. Moreover, we show that this lemma includes the reduction modulo Φ_{p^e} we are looking for. We start by defining a set of polynomials $\tau_0, \tau_{\ell,b} \in \mathbb{F}_q[x]$ for $0 < \ell < e$ and $b \in \pi_{p^\ell}(\mathcal{K})$. Since we are still working in the ring $\mathbb{F}_q[x]/(x^{p^e} - 1)$, we assume all polynomials to be reduced modulo $x^{p^e} - 1$, that is, we identify $(a \bmod p^e) \in \mathbb{Z}_{p^e}^\times$ with its canonical representative $\bar{a} \in \mathbb{Z}$, $0 < \bar{a} < p^e$, such that $\bar{a} \equiv a \bmod p^e$. For $0 < \ell < e$, $0 \le i < n_{\ell+1}/n_\ell$, and $b \in \pi_{p^\ell}(\mathcal{K})$, we consider

$$\mathcal{I}_{\ell,b,i} = \{a \in \pi_{p^{\ell+1}}(\mathcal{K}) \colon a \equiv q^{-in_\ell} b \bmod p^\ell\},$$

the set of all elements in $\pi_{p^{\ell+1}}(\mathcal{K})$ that are preimages of $q^{-in_\ell}b$ under the canonical projection $\pi \colon \mathbb{Z}_{p^{\ell+1}}^\times \to \mathbb{Z}_{p^\ell}^\times$. For $0 < \ell < e$ and $b \in \pi_{p^\ell}(\mathcal{K})$, we set

$$\begin{aligned} \tau_0 &= \textstyle\sum_{0 \le i < n_1} \sum_{a \in \pi_p(\mathcal{K})} (x^{p^{e-1}})^{aq^i} + 1 \in \mathbb{F}_q[x] \qquad \text{and} \\ \tau_{\ell,b} &= \textstyle\sum_{0 \le i < \frac{n_{\ell+1}}{n_\ell}} \sum_{a \in \mathcal{I}_{\ell,b,i}} \sum_{0 \le s < \ell+1} (x^{p^{e-(\ell+1)}})^{ap^s q^{in_\ell}} \\ &\quad -p \cdot \textstyle\sum_{0 \le s < \ell} (x^{p^{e-\ell}})^{bp^s} \in \mathbb{F}_q[x]. \end{aligned} \tag{4.12}$$

PROPOSITION 4.13. *For $0 < \ell < e$, let τ_0 and $\tau_{\ell,b}$ be the polynomials as in (4.12) for all $b \in \pi_{p^\ell}(\mathcal{K})$. Then Φ_{p^e} divides τ_0 and $\tau_{\ell,b}$.*

PROOF. Fix $0 < \ell < e$, and let $\pi \colon \mathbb{Z}_{p^{\ell+1}}^\times \to \mathbb{Z}_{p^\ell}^\times$ with $\pi(a) = (a \bmod p^\ell)$ the canonical projection from $\mathbb{Z}_{p^{\ell+1}}^\times$ onto $\mathbb{Z}_{p^\ell}^\times$. Since we have $\pi_{p^\ell} = \pi \circ \pi_{p^{\ell+1}}$, the projection is a surjective homomorphism. Thus, each element $b \in \mathbb{Z}_{p^\ell}^\times$ has a preimage set $\pi^{-1}(b) = \{a \in \mathbb{Z}_{p^{\ell+1}}^\times \colon a \equiv b \bmod p^\ell\}$ of order $\#\pi^{-1}(b) =$

$\frac{\#\mathbb{Z}^\times_{p^{\ell+1}}}{\#\mathbb{Z}^\times_{p^\ell}} = \frac{p^\ell(p-1)}{p^{\ell-1}(p-1)} = p$. One can easily check that the kernel of π is $\ker\pi = \{(1+p^\ell z) \bmod p^{\ell+1} \colon 0 \le z < p\}$. This gives a second way to express the preimage set of b in $\mathbb{Z}^\times_{p^{\ell+1}}$:

$$\pi^{-1}(b) = b \cdot \ker\pi = \{(b + zp^\ell) \bmod p^{\ell+1} \colon 0 \le z < p\}. \tag{4.14}$$

Here we use that the map $\psi_b \colon \{0,\dots,p-1\} \to \{0,\dots,p-1\}$ with $\psi_b(z) = bz \operatorname{rem} p$ is a permutation because $\gcd(b,p) = 1$.

We can also give a description of $\pi^{-1}(b)$ involving $\mathcal{I}_{\ell,b,i}$. Since we know that $q^{n_\ell} \in \pi_{p^\ell}(\mathcal{K})$, also the inverse of q^{in_ℓ} is an element in $\pi_{p^\ell}(\mathcal{K})$. Thus, the set $\mathcal{I}_{\ell,b,i}$ contains $\frac{k_{\ell+1}}{k_\ell}$ elements. For $0 < i < \frac{n_{\ell+1}}{n_\ell}$ and $a \in \mathcal{I}_{\ell,b,i}$, we have $\pi(q^{in_\ell} \cdot a) \equiv q^{in_\ell} \cdot q^{-in_\ell} b \equiv b \bmod p^\ell$. Hence, the set $\{q^{in_\ell} a \colon 0 \le i < \frac{n_{\ell+1}}{n_\ell} \text{ and } a \in \mathcal{I}_{\ell,b,i}\}$ is a subset of $\pi^{-1}(b)$. But $\biguplus_{0\le i<n_{\ell+1}} q^i \pi_{p^{\ell+1}}(\mathcal{K})$ is a partition of $\mathbb{Z}^\times_{p^{\ell+1}}$, and each subset has $\frac{n_{\ell+1}}{n_\ell} \cdot \frac{k_{\ell+1}}{k_\ell} = \frac{\phi(p^{\ell+1})}{\phi(p^\ell)} = p$ different elements. Therefore, equality holds:

$$\pi^{-1}(b) = \left\{ q^{in_\ell} a \colon 0 \le i < \frac{n_{\ell+1}}{n_\ell} \text{ and } a \in \mathcal{I}_{\ell,b,i} \right\}. \tag{4.15}$$

With the help of these formulas we have for $0 < \ell < e$ and all $b \in \pi_{p^\ell}(\mathcal{K})$:

$$\begin{aligned}
&\sum_{0\le i<\frac{n_{\ell+1}}{n_\ell}} \sum_{\substack{a\in\mathcal{I}_{\ell,b,i}\\ 0\le s<\ell+1}} (x^{p^{e-(\ell+1)}})^{aq^{in_\ell}p^s} \\
&\overset{(4.15)}{\equiv} \sum_{\substack{a\in\pi^{-1}(b)\\ 0\le s<\ell+1}} (x^{p^{e-(\ell+1)}})^{ap^s} \overset{(4.14)}{\equiv} \sum_{\substack{0\le z<p\\ 0\le s<\ell+1}} (x^{p^{e-(\ell+1)}})^{p^s(b+zp^\ell)} \\
&\equiv \sum_{0\le s<\ell+1} \left((x^{p^{e-(\ell+1)}})^{bp^s} \cdot \left(\sum_{0\le z<p} (x^{p^{e-1}})^{zp^s} \right) \right) \bmod (x^{p^e}-1)
\end{aligned}$$

For $s = 0$, the sum in the inner brackets vanishes modulo Φ_{p^e} since

$$\sum_{0\le z<p} (x^{p^{e-1}})^z = \frac{x^{p^e}-1}{x^{p^{e-1}}-1} \equiv 0 \bmod \Phi_{p^e}.$$

For $s \ge 1$, we simplify modulo Φ_{p^e}:

$$\sum_{0\le z<p} (x^{p^{e-1}})^{zp^{1+(s-1)}} \equiv \sum_{0\le z<p} 1^{zp^{s-1}} \equiv p \bmod \Phi_{p^e}.$$

Inserting both formulas gives

$$\begin{aligned}
&\sum_{0\le i<\frac{n_{\ell+1}}{n_\ell}}\sum_{a\in\mathcal{I}_{\ell,b,i}}\sum_{0\le s<\ell+1}(x^{p^{e-(\ell+1)}})^{ap^sq^{in_\ell}}\\
&\equiv(x^{p^{e-(\ell+1)}})^{bp^0}\cdot 0+\sum_{1\le s<\ell+1}(x^{p^{e-(\ell+1)}})^{bp^s}\cdot p\\
&\equiv p\cdot\sum_{0\le s<\ell}(x^{p^{e-\ell}})^{bp^s}\bmod\Phi_{p^e}. \qquad (4.16)
\end{aligned}$$

It follows by construction of $\tau_{\ell,b}$ in (4.12) that Φ_{p^e} is a divisor of $\tau_{\ell,b}$ for $0<\ell<e$ and $b\in\pi_{p^\ell}(\mathcal{K})$. For τ_0 we have

$$\begin{aligned}
\sum_{\substack{a\in\pi_p(\mathcal{K})\\0\le i<n_1}}(x^{p^{e-1}})^{aq^i}&=\sum_{a\in\mathbb{Z}_p^\times}(x^{p^{e-1}})^a\\
&=\sum_{0\le z<p}(x^{p^{e-1}})^z-1=\frac{x^{p^e}-1}{x^{p^{e-1}}-1}-1\equiv-1\bmod\Phi_{p^e},
\end{aligned}$$

since $\langle q,\pi_p(\mathcal{K})\rangle=\mathbb{Z}_p^\times$, and the claim follows also for τ_0. □

Let $\zeta^{p^{e-\ell}}=\zeta_\ell$ be a primitive p^ℓth root of unity for $0\le\ell<e$. Since $e-\ell\ge1$ and $(\zeta_\ell)^{p^{e-1}}=\zeta^{p^{e-\ell+e-1}}=1$, a simple computation gives

$$\tau_0(\zeta_\ell)=\sum_{a\in\pi_p(\mathcal{K})}\sum_{0\le i<n_1}(\zeta_\ell^{p^{e-1}})^{aq^i}+1=n_1k_1+1=\phi(p)+1=p\neq0\text{ in }\mathbb{F}_q.$$

Thus, $\gcd(\tau_0,\Phi_{p^\ell})=1$ for $0\le\ell<e$ and for all $b\in\pi_{p^\ell}(\mathcal{K})$ we have

$$\gcd(\tau_0,\tau_{1,b},\dots,\tau_{e-1,b},x^{p^e}-1)=\Phi_{p^e}\text{ in }\mathbb{F}_q[x]. \qquad (4.17)$$

Since $q^{in_\ell}\in\pi_{p^\ell}(\mathcal{K})$, we can write $\pi^{-1}(\pi_{p^\ell}(\mathcal{K}))$ as

$$\pi^{-1}(\pi_{p^\ell}(\mathcal{K}))=\pi_{p^{\ell+1}}(\mathcal{K})=\biguplus_{0\le i<\frac{n_{\ell+1}}{n_\ell}}\biguplus_{b\in\pi_{p^\ell}(\mathcal{K})}\mathcal{I}_{\ell,b,i}.$$

A direct consequence is that for $0<\ell<e$

$$\begin{aligned}
\tau_\ell=\;&\textstyle\sum_{0\le i<\frac{n_{\ell+1}}{n_\ell}}\sum_{a\in\pi_{p^{\ell+1}}(\mathcal{K})}\sum_{0\le s<\ell+1}(x^{p^{e-(\ell+1)}})^{ap^sq^{in_\ell}}\\
&-p\cdot\textstyle\sum_{b\in\pi_{p^\ell}(\mathcal{K})}\sum_{0\le s<\ell}(x^{p^{e-\ell}})^{bp^s}
\end{aligned} \qquad (4.18)$$

is divisible by Φ_{p^e}.

Remark 4.19. *Successively applying (4.12) and (4.18), respectively, we can transform the equation given in Lemma 4.5 into*

$$\left(\sum_{a\in\mathcal{K}}\sum_{0\le s<e}x^{ap^sq^i}\right)\cdot\left(\sum_{b\in\mathcal{K}}\sum_{0\le s'<e}x^{bp^{s'}}\right)\equiv\sum_{0\le h<n}C'_{e,h}\cdot\left(\sum_{a\in\mathcal{K}}\sum_{0\le s<e}x^{ap^s}\right)^{q^h}\bmod\Phi_{p^e}$$

where $C'_{e,h}$ depends on $0 \le i < n$.

This is indeed a way to compute a suitable preimage of $\varphi(A) \cdot \varphi(B)$ in $\mathcal{R} = \mathbb{F}_q[x]/(\Phi_{p^e})$. We observe that the final formula is due to a basis of $\mathcal{R}$ which supports the back-transformation into a linear combination of the conjugates of a normal Gauß period α.

LEMMA 4.20. *Let $\zeta = (x \bmod \Phi_{p^e})$ and $\mathcal{R} = \mathbb{F}_q[x]/(\Phi_{p^e})$. If $\mathbb{Z}_{p^e}^\times = \langle q, \mathcal{K} \rangle$ for a subgroup $\mathcal{K}$ of $\mathbb{Z}_{p^e}^\times$ then*

$$\mathcal{B} = \left\{ \sum_{0 \le s < e} \zeta^{ap^s} : a \in \mathbb{Z}_{p^e}^\times \right\}$$

is a basis of $\mathcal{R}$.

PROOF. The set $\mathcal{B}' = \{1, \zeta, \ldots, \zeta^{\phi(p^e)-1}\}$ is a basis of $\mathcal{R}$. Since $\mathcal{B}$ has at most $\#\mathcal{B}' = \phi(p^e)$ elements, it is sufficient to prove that $\mathcal{B}' \subseteq \langle \mathcal{B} \rangle$.

By construction, we have $\sum_{0 \le s < e} \zeta^{ap^s} \in \langle \mathcal{B} \rangle$ for $a \in \mathbb{Z}_{p^e}^\times$. By induction on ℓ, we find with Proposition 4.13 that for $0 < \ell < e$ we have $\sum_{0 \le s < \ell} (\zeta^{p^{e-\ell}})^{ap^s} \in \langle \mathcal{B} \rangle$ for $a \in \mathbb{Z}_{p^\ell}^\times$, since $\tau_{\ell,b}(\zeta) = 0$. Furthermore, we have $-1 \in \langle \mathcal{B} \rangle$.

Now let $1 \le a < \phi(p^e)$. Then there exist uniquely determined $0 < \ell \le e$ and $c \in \mathbb{Z}_{p^\ell}^\times$ such that $a \equiv p^{e-\ell} c \bmod p^e$, and

$$\sum_{0 \le s < \ell} (\zeta^{p^{e-\ell}})^{cp^s} = \zeta^{cp^{e-\ell}} + \sum_{1 \le s < \ell} (\zeta^{p^{e-\ell}})^{cp^s} = \zeta^{cp^{e-\ell}} + \sum_{0 \le s < \ell-1} (\zeta^{p^{e-(\ell+1)}})^{cp^s}.$$

But both $\sum_{0 \le s < \ell} (\zeta^{p^{e-\ell}})^{cp^s}$ and $\sum_{0 \le s < \ell-1} (\zeta^{p^{e-\ell+1}})^{cp^s}$ are elements of $\langle \mathcal{B} \rangle$. Hence, $\zeta^{cp^{e-\ell}} = \zeta^a \in \langle \mathcal{B} \rangle$ for all $0 \le a < \phi(p^e)$, and the claim follows. □

Now we translate this result into the language of traces that has motivated the choice of $\tau_{\ell,b}$. Let $\mathrm{Tr}_{q^{n_\ell}/q^{n_{\ell-1}}}$ be the trace map of $\mathbb{F}_{q^{n_\ell}}$ into $\mathbb{F}_{q^{n_{\ell-1}}}$ for $0 < \ell \le e$; here $n_0 = 1$ by definition. We have

$$\mathrm{Tr}_{q^{n_\ell}/q^{n_{\ell-1}}}(\alpha_\ell) = \sum_{0 \le i < n_\ell / n_{\ell-1}} \alpha_\ell^{q^{i n_{\ell-1}}}.$$

Since ζ is a root of Φ_{p^e}, we can apply (4.18) to $\alpha_\ell = \sum_{\substack{a \in \pi_{p^\ell} \mathcal{K} \\ 0 \le s < \ell}} (\zeta^{p^{e-\ell}})^{ap^s}$. Then

$$\mathrm{Tr}_{q^{n_{\ell+1}}/q^{n_\ell}}(\alpha_{\ell+1}) = p\alpha_\ell \text{ for all } 1 \le \ell < e. \tag{4.21}$$

For τ_0, we simply have $\tau_0(\zeta) = 0$ and

$$\mathrm{Tr}_{q^{n_1}/q}(\alpha_1) = -1. \tag{4.22}$$

The trace map is transitive, so that $\mathrm{Tr}_{q^n/q^{n_\ell}}(\alpha) = \mathrm{Tr}_{q^{n_{\ell+1}}/q^{n_\ell}}(\mathrm{Tr}_{q^n/q^{n_{\ell+1}}}(\alpha))$. We use this to prove Lemma 4.11 by induction on $0 \le \ell \le e$. The case $\ell = 0$ is also called the *absolute trace*.

PROOF (of Lemma 4.11). For $\ell = e$, we have $\mathrm{Tr}_{q^n/q^{n_e}}(\alpha) = \mathrm{Tr}_{q^{n_e}/q^{n_e}}(\alpha) = \alpha_e$ since $n = n_e$. Now we suppose that the claim is true for an $1 < \ell < e$. Then

$$\begin{aligned}\mathrm{Tr}_{q^n/q^{n_\ell}}(\alpha_{\ell+1}) &= \mathrm{Tr}_{q^{n_{\ell+1}}/q^{n_\ell}}(p^{e-(\ell+1)}\alpha_{\ell+1}) \\ &= p^{e-(\ell+1)}\mathrm{Tr}_{q^{n_{\ell+1}}/q^{n_\ell}}(\alpha_{\ell+1}) \overset{(4.21)}{=} p^{e-(\ell+1)}(p\alpha_\ell).\end{aligned}$$

For $\ell = 0$ we get $\mathrm{Tr}_{q^n/q}(\alpha) = p^{e-1}\mathrm{Tr}_{q^{n_1}/q}(\alpha_1) \overset{(4.22)}{=} -p^{e-1}$ in the same way. □

We finally rewrite Remark 4.19 inserting the root ζ of Φ_{p^e}.

REMARK 4.23. *The primitive p^eth root of unity ζ is a zero of Φ_{p^e}, and we have*

$$\alpha^{q^i} \cdot \alpha = \sum_{0 \le h < n} C'_{e,h}\alpha^{q^h}$$

for all $0 \le i < n$. The $C'_{e,h}$ depend on the given $0 \le i < n$. They are elements of the prime subfield $\mathbb{F}$ of $\mathbb{F}_q$ because $C^{(i)}_{p^{e-\ell}q^h} \in \mathbb{F}$ by Lemma 4.5 and all manipulations on the coefficients are done in $\mathbb{F}$. Thus, the multiplication matrix $T_{\mathcal{N}}$ has entries in $\mathbb{F}$.

4.1.3 The complete algorithm.

We have presented all parts of the algorithm, and now summarize the complete multiplication routine.

ALGORITHM 4.24. The prime power case.
Input: A normal prime power Gauß period α of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ with $\mathcal{K}$ a subgroup of $\mathbb{Z}^\times_{p^e}$ of order k, and two elements $A = \sum_{0 \le i < n} A_i\alpha^{q^i}$ and $B = \sum_{0 \le i < n} B_i\alpha^{q^i}$ of $\mathbb{F}_{q^n}$ with coefficients $A_i, B_i \in \mathbb{F}_q$ for $0 \le i < n$.
Output: The product $C = \sum_{0 \le i < n} C_i\alpha^{q^i}$ of A and B with coefficients $C_i \in \mathbb{F}_q$ for $0 \le i < n$.

Transformation from $\mathbb{F}_{q^n}$ into $\mathbb{F}_q[x]/(x^{p^e} - 1)$:
1. $A'_j \leftarrow 0$ and $B'_j \leftarrow 0$ for all $0 < j < p^e$.
2. For all $0 \le i < n$ and $a \in \mathcal{K}$ do set $j = aq^i \operatorname{rem} p^e$ and $A'_j \leftarrow A_i$ and $B'_j \leftarrow B_i$.
3. For $0 < \ell < e$ and all $i \in \mathbb{Z}^\times_{p^{e-(\ell-1)}}$ do
4. set $j = i \cdot p^\ell \operatorname{rem} p^e$ and $A'_j \leftarrow A'_j + A'_i$, $B'_j \leftarrow B'_j + B'_i$.
5. Set $A' = \sum_{1 \le j < p^e} A'_j x^j$ and $B' = \sum_{1 \le j < p^e} B'_j x^j$.

Multiplication in $\mathbb{F}_q[x]/(x^{p^e} - 1)$:

6. Compute $C' = \sum_{2 \le j < 2p^e-1} C'_j x^j \leftarrow A' \cdot B'$ with (fast) polynomial multiplication in $\mathbb{F}_q[x]$.
7. Reduce C' modulo $x^{p^e} - 1$: For $2 \le j < p^e - 1$ do $C'_j \leftarrow C'_j + C'_{j+p^e}$. Set $C'_0 = C'_{p^e}$, $C'_1 = C'_{p^e+1}$, $C' = \sum_{0 \le j < p^e} C'_j x^j$.
   Write the product as a sum of Gauß periods in $\mathbb{F}_q[x]/(x^{p^e} - 1)$*:*
8. Set $C_0 = C'_0$.
9. For all $0 < \ell \le e$ and $0 \le h < n$ do $D^{(\ell)}_{\ell,h} \leftarrow 0$ and $C_{e,h} \leftarrow C'_{q^h}$.
10. For ℓ from $e-1$ down to 1 do 11–14
11. For $0 \le h < n_\ell$ do
12. $D^{(\ell)}_{\ell,h} \leftarrow \frac{k_{\ell+1}}{k_\ell} \cdot \sum_{0 \le j < \frac{n_{\ell+1}}{n_\ell}} (D^{(\ell+1)}_{\ell+1,h+jn_\ell} + C_{\ell+1,h+jn_\ell})$.
13. For $0 \le h < n_\ell$ do
14. $C_{\ell,h} \leftarrow C'_{p^{e-\ell}q^h} - D^{(\ell)}_{\ell,h}$.
15. Set $C'' = C_0 + \sum_{0<\ell\le e} \sum_{0 \le h < n_\ell} C_{\ell,h} \left(\sum_{a \in \pi_{p^\ell}(\mathcal{K})} \sum_{0 \le s < \ell} (x^{p^{e-\ell}})^{ap^s} \right)^{q^h} \bmod (x^{p^e} - 1)$.
   Reduction modulo $\Phi_{p^e} \in \mathbb{F}_q[x]$ *applying the trace map:*
16. For $0 \le h < n_1$ do $C_{1,h} \leftarrow C_{1,h} - C_0$.
17. For $1 \le \ell < e$ and $0 \le h < n_\ell$ do
18. For $0 \le i < \frac{n_{\ell+1}}{n_\ell}$ do $C_{\ell+1,h+in_\ell} \leftarrow C_{\ell+1,h+in_\ell} + p^{-1} \cdot C_{\ell,h}$.
   Back transformation from $\mathcal{R} = \mathbb{F}_q[x]/(\Phi_{p^e})$ *into* $\mathbb{F}_{q^n}$*:*
19. For $0 \le h < n$ do set $C_h = C_{e,h}$.
20. Return $C = \sum_{0 \le h < n} C_h \alpha^{q^h}$.

LEMMA 4.25. *Algorithm 4.24 works as specified.*

PROOF. The computation of the transformation in steps 1–5 follows the definition of Gauß periods. The multiplication in steps 6–7 in $\mathbb{F}_q[x]/(x^{p^e} - 1)$ generates a preimage of the product of $A \cdot B$. To compute the reduction modulo Φ_{p^e}, we apply the reordering of the summands according to Proposition 4.10 in steps 8–15. Notice that we compute only the $D^{(\ell)}_{\ell,h}$ for $1 \le \ell < e$ according to Lemma 4.9(iii). These are sufficient to get all coefficients of Lemma 4.5, see (4.8). The reduction in steps 16–18 is done according to (4.12) and (4.18), respectively. Thus, we get the preimage of $A \cdot B$ in the ring $\mathcal{R} = \mathbb{F}_q[x]/(\Phi_{p^e})$ under the isomorphism χ as stated in Remark 4.19. The final back transformation (steps 19–20) uses the fact that C is a linear combination of the conjugates of α as claimed in Remark 4.23. □

It remains to count the number of operations in $\mathbb{F}_q$. $\mathsf{M}(n)$ denotes a multiplication time, so that two polynomials in $\mathbb{F}_q[x]$ of degree at most n can be multiplied with $O(\mathsf{M}(n))$ operations in $\mathbb{F}_q$. We may use $\mathsf{M}(n) = n \log n \log\log n$ by Schönhage & Strassen (1971) and Schönhage (1977); see also Cantor (1989). We recall that $n_\ell \le \phi(p^\ell)$ for $1 \le \ell \le e$. Furthermore, the telescoping sum

below is useful:

$$\sum_{1\le\ell\le e}\phi(p^\ell)=\sum_{1\le\ell\le e}(p^\ell-p^{\ell-1})=p^e+\sum_{1\le\ell<e}p^\ell-\sum_{1\le\ell<e}p^\ell-p^0=p^e-1.$$

We have the following estimates for each part of the algorithm. We emphasize the prime case $e=1$ since some steps are omitted in this special situation.

- The transformation (steps 1–5) is calculated with 2 additions for each $i\in\mathbb{Z}^\times_{p^{e-(\ell-1)}}$ where $0<\ell<e$. This results in a total of at most

$$\sum_{0<\ell<e}2\phi(p^{e-(\ell-1)})=2\sum_{2\le\ell\le e}\phi(p^\ell)=2(p^e-1-\phi(p))=2p^e-2p$$

  operations in $\mathbb{F}_q$. For the prime case $e=1$ we have $2(p^e-p)=0$ operations.
- Since both A' and B' have constant coefficient zero, the multiplication modulo $x^{p^e}-1$ in steps 6–7 can be done with

$$\mathsf{M}(p^e-1)+(p^e-3)$$

  operations. The second term counts the additions. If $e=1$ then $p-1=\phi(p)=nk$.
- The sorting of the summands in steps 8–15 is omitted for the prime case $e=1$. Otherwise $e\ge 2$ and we may assume that $k_{\ell+1}/k_\ell$ is precomputed for all $0<\ell<e$. Then the number of operations is bounded by

$$\begin{aligned}&\sum_{\substack{1\le\ell<e\\0\le h<n_\ell}}\left(1+\frac{n_{\ell+1}}{n_\ell}-1+\sum_{0\le i<\frac{n_{\ell+1}}{n_\ell}}1+1\right)\\&=2\sum_{1\le\ell<e}n_{\ell+1}+\sum_{1\le\ell<e}n_\ell\le 2\sum_{2\le\ell\le e}\phi(p^\ell)+\sum_{1\le\ell<e}\phi(p^\ell)\\&=2(p^e-p)+p^{e-1}-1.\end{aligned}$$

- The trace is applied in steps 16–18. Step 16 is executed for all $e\ge 1$ with $n_1\le p-1$ operations. For $e=1$, we have $n_1=n$. If $e\ge 2$ the subsequent iterative computation of the trace map in steps 17–18 can be done with

$$\sum_{\substack{1\le\ell<e\\0\le h<n_\ell}}\sum_{0\le i<\frac{n_{\ell+1}}{n_\ell}}2=2\sum_{2\le\ell\le e}n_\ell\le 2\sum_{2\le\ell\le e}\phi(p^\ell)=2(p^e-p)$$

  further operations if we suppose p^{-1} to be precomputed.
- The back-transformation (steps 19–20) can be done without operations in $\mathbb{F}_q$.

We summarize this detailed cost analysis in the next theorem.

THEOREM 4.26. *Let q be a prime power coprime to a prime p, and e a positive integer such that there exists a normal Gauß period α of type $(n, \mathcal{K})$ over $\mathbb{F}_q$, where $\mathcal{K}$ is a subgroup of $\mathbb{Z}_{p^e}^\times$. In the normal basis representation with respect to $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n-1}})$, two elements of $\mathbb{F}_q$ can be multiplied with at most*

$$\mathsf{M}(p^e - 1) + 7p^e + p^{e-1} - 6p - 4 + n \leq \mathsf{M}(p^e) + 8p^e \in O(\mathsf{M}(p^e))$$

operations in $\mathbb{F}_q$.

We remark that all divisions in the algorithm (steps 12 and 18) are performed in the prime subfield of $\mathbb{F}_{q^n}$. The only operations that are performed in $\mathbb{F}_q$ are additions, subtractions, and multiplications.

The result of Gao *et al.* (1995, 2000) for the prime case $kn = \varphi(p) = \varphi(p^e)$ is a corollary.

COROLLARY 4.27 (Gao *et al.* 2000, Theorem 4.1). *Let $\mathbb{F}_{q^n}$ be given by a normal basis $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n-1}})$, where α is a prime Gauß period of type (n, k) over $\mathbb{F}_q$. Then two elements of $\mathbb{F}_q$ given as a linear combination of the basis elements can be multiplied with at most*

$$\mathsf{M}(kn) + (k+1)n - 3$$

operations in $\mathbb{F}_q$.

5 Decomposable Gauß periods

The main work in our connection between polynomial arithmetic and Gauß periods is for a special case, namely *decomposable Gauß periods*, the topic of this section. The general case is dealt with later.

Let α be a normal Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ and $r = r_1 \cdots r_t$ the prime power decomposition as in (2.2), so that

$$\mathbb{Z}_r^\times \cong \mathbb{Z}_{r_1}^\times \times \cdots \times \mathbb{Z}_{r_t}^\times,$$

$$\mathcal{K} \subseteq \pi_{r_1}(\mathcal{K}) \times \cdots \times \pi_{r_t}(\mathcal{K}). \tag{5.1}$$

Sometimes, $\mathcal{K}$ equals this direct sum of its projections.

EXAMPLE 2.5 CONTINUED. (iii) Recall the two subgroups

$$\mathcal{K}_1 = \{1, 26\} \cong \{1, 8\} \times \{1\} = \pi_9(\mathcal{K}_1) \times \pi_5(\mathcal{K}_1),$$
$$\mathcal{K}_2 = \{1, 44\} \neq \{1, 19, 26, 44\} \cong \{1, 8\} \times \{1, 4\} = \pi_9(\mathcal{K}_2) \times \pi_5(\mathcal{K}_2)$$

of $\mathbb{Z}_{45}^\times$. Both generate normal Gauß periods in $\mathbb{F}_{2^{12}}$ over $\mathbb{F}_2$. Thus $\mathcal{K}_1$ is the direct sum of its projected images while $\mathcal{K}_2$ is not. $\Diamond$

DEFINITION 5.2. *Let $r \geq 2$ be an integer with prime power decomposition $r = r_1 \cdots r_t$, and let $\mathcal{K}$ be a subgroup of $\mathbb{Z}_r^\times$.*

(i) Let $\pi_{r_i} \colon \mathbb{Z}_r^\times \to \mathbb{Z}_{r_i}^\times$ for $1 \leq i \leq t$ be the canonical projection. The subgroup $\mathcal{K}$ is called decomposable *if*

$$\mathcal{K} \cong \pi_{r_1}(\mathcal{K}) \times \cdots \times \pi_{r_t}(\mathcal{K}).$$

(ii) A Gauß period α of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ is decomposable *if and only if $\mathcal{K}$ is decomposable.*

Let R_1 be the squarefree part of r as in Definition 2.3. We call a Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ with $\mathcal{K} \subseteq \mathbb{Z}_r^\times$ *squarefree* if $r = R_1$. If $\mathcal{K}$ is decomposable, then we can factor the normal Gauß period α. For squarefree r, this (and also Proposition 5.4 below) is in Gao (2001), Theorem 1.5.

LEMMA 5.3. *Let α be a decomposable normal Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ given by ζ, $r = r_1 \cdots r_t$ the prime power decomposition, and for $1 \leq i \leq t$ let α_i be the Gauß period of type $(n_i, \pi_{r_i}(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to $\zeta_i = \zeta^{r/r_i}$, where $n_i = \phi(r_i)/\#\pi_{r_i}(\mathcal{K})$. Then there exist $h_1, \ldots, h_t$ with $0 \leq h_i < n_i$ for $i \leq t$ and such that*

$$\alpha = \prod_{1 \leq i \leq t} \alpha_i^{q^{h_i}}.$$

Before we give the proof, we illustrate it by an example.

EXAMPLE 2.5 CONTINUED. (iii) Let ζ be a primitive 45th root of unity. The normal Gauß period $\alpha = \zeta^{14} + \zeta^{24} + \zeta^4 + \zeta^{39}$ of type $(12, \{1, 26\})$ with $\{1, 26\} \subset \mathbb{Z}_{45}^\times$ is decomposable. The canonical projections along the prime power decomposition of $45 = 3^2 \cdot 5$ generate the prime Gauß period $\alpha_5 = \zeta^9$ of type $(4, \{1\})$ and the prime power Gauß period $\alpha_9 = \zeta^5 + (\zeta^5)^3 + (\zeta^5)^8 + (\zeta^5)^6$ of type $(3, \{1, 8\})$ over $\mathbb{F}_2$. Computing the product $\alpha_5 \cdot \alpha_9 = \zeta^9 \cdot (\zeta^5 + \zeta^{15} + \zeta^{40} + \zeta^{30}) = \zeta^{14} + \zeta^{24} + \zeta^4 + \zeta^{39}$ verifies that $\alpha_5 \cdot \alpha_9$ is indeed a factorization of α. $\Diamond$

PROOF. We divide the proof into three steps. Since α is normal, we have $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$ by Theorem 2.6.

CLAIM. *A decomposable normal Gauß period can be written as a product of a squarefree Gauß period and a non-squarefree Gauß period.*

Let R_1 be the squarefree part of r and $R_2 = \frac{r}{R_1}$, and set $a_i \equiv a \bmod R_i$ for $i = 1, 2$. For a primitive rth root of unity ζ, we have $\zeta_i = \zeta^{r/R_i}$ a primitive R_ith root of unity for $i = 1, 2$. Hence, $\zeta_1^a = \zeta_1^{a_1}$ and $\zeta_2^a = \zeta_2^{a_2}$. Because $\mathcal{K}$ is decomposable, we have the direct sum $\mathcal{K} = \pi_{R_1}(\mathcal{K}) \times \pi_{R_2}(\mathcal{K})$. By a straightforward computation we have:

$$\begin{aligned}
\alpha &= \sum_{a \in \mathcal{K}} b(\zeta^a) = \sum_{a \in \mathcal{K}} \zeta^{R_2 a} \cdot \prod_{1 \le i \le t, p_i \mid R_2} \sum_{1 \le s \le e_i} \zeta^{a R_1 R_2 / p_i^s} \\
&= \sum_{(a_1, a_2) \in \pi_{R_1}(\mathcal{K}) \times \pi_{R_2}(\mathcal{K})} (\zeta^{r/R_1})^{a_1} \cdot \prod_{1 \le i \le t, p_i \mid R_2} \sum_{1 \le s \le e_i} (\zeta^{r/R_2})^{a_2 R_2 / p_i^s} \\
&= \sum_{(a_1, a_2) \in \pi_{R_1}(\mathcal{K}) \times \pi_{R_2}(\mathcal{K})} b(\zeta_1^{a_1}) \cdot b(\zeta_2^{a_2}) \\
&= \sum_{a_1 \in \pi_{R_1}(\mathcal{K})} b(\zeta_1^{a_1}) \cdot \sum_{a_2 \in \pi_{R_2}(\mathcal{K})} b(\zeta_2^{a_2}).
\end{aligned}$$

The first factor is a squarefree Gauß period of type $\left(\frac{\phi(R_1)}{\#\pi_{R_1}(\mathcal{K})}, \pi_{R_1}(\mathcal{K})\right)$ over $\mathbb{F}_q$ with respect to $\zeta_1 = \zeta^{r/R_1}$, the second one is a non-squarefree Gauß period. This proves the claim.

Claim. *A decomposable non-squarefree Gauß period which is not a prime power Gauß period can be written as a product of a non-squarefree Gauß period and a prime power Gauß period.*

Let α be a non-squarefree Gauß period. Since it is not a prime power Gauß period, we have $t \ge 2$. Set $R = r_1 \cdots r_{t-1} \ge 2$. Then $r_t \ge 2$ is a prime power coprime to R. For a primitive rth root of unity ζ, we have $\zeta_1 = \zeta^{r_t} = \zeta^{r/R}$ a primitive Rth root of unity, and $\zeta_2 = \zeta^R = \zeta^{r/r_t}$ is a primitive r_tth root of unity. Let $a_1 \equiv a \bmod R$ and $a_2 \equiv a \bmod r_t$. Then

$$\begin{aligned}
\alpha &= \sum_{a \in \mathcal{K}} b(\zeta^a) = \sum_{a \in \mathcal{K}} \prod_{1 \le i \le t} \sum_{1 \le s \le e_i} \zeta^{ar/p_i^s} \\
&= \sum_{a \in \mathcal{K}} \prod_{1 \le i \le t, p_i \mid R} \sum_{1 \le s \le e_i} (\zeta^{r_t})^{aR/p_i^s} \cdot \prod_{1 \le i \le t, p_i \mid r_t} \sum_{1 \le s \le e_i} (\zeta^R)^{ar_t/p_i^s} \\
&= \sum_{(a_1, a_2) \in \pi_R(\mathcal{K}) \times \pi_{r_t}(\mathcal{K})} \left(\prod_{1 \le i \le t, p_i \mid R} \sum_{1 \le s \le e_i} (\zeta_1)^{a_1 R/p_i^s} \cdot \prod_{1 \le i \le t, p_i \mid r_t} \sum_{1 \le s \le e_i} (\zeta_2)^{a_2 r_t/p_i^s} \right) \\
&= \sum_{a_1 \in \pi_R(\mathcal{K})} b(\zeta_1^{a_1}) \cdot \sum_{a_2 \in \pi_{r_t}(\mathcal{K})} b(\zeta_2^{a_2}),
\end{aligned}$$

with the first factor a non-squarefree Gauß period and the second one a prime power Gauß period. This shows the claim.

Claim. *A squarefree Gauß period which is not a prime Gauß period can be written as a product of (conjugates of) a squarefree Gauß period and a prime Gauß period.*

Let ζ be a primitive rth root of unity, and let $R = r_1 \cdots r_{t-1}$, which is greater than 1 and coprime to r_t. Let $\zeta_1 = \zeta^{r_t}$ be a primitive Rth root of unity and $\zeta_2 = \zeta^R$ a primitive r_tth root of unity, and $u_1, u_2 \in \mathbb{Z}$ such that $u_1 r_t + u_2 R = 1$; we can find these by the Extended Euclidean Algorithm. Let a_1 and a_2 be the projections of a onto $\mathbb{Z}_R^\times$ and $\mathbb{Z}_{r_t}^\times$, respectively, and set $n_1 = \frac{\phi(R)}{\#\pi_R(\mathcal{K})}$ and $n_2 = \frac{\phi(r_t)}{\#\pi_{r_t}(\mathcal{K})}$. Since α is normal, we have $\langle q, \pi_R(\mathcal{K})\rangle = \mathbb{Z}_R^\times$ and $\langle q, \pi_{r_t}(\mathcal{K})\rangle = \mathbb{Z}_{r_t}^\times$. Thus, there are $0 \le h_1 < n_1$ and $0 \le h_2 < n_2$ such that $u_1 \in q^{h_1}\pi_R(\mathcal{K})$ and $u_2 \in q^{h_2}\pi_{r_t}(\mathcal{K})$. The first factor is a squarefree Gauß period of type $(n_1, \pi_R(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to $\zeta^{r/R}$, and the second factor is a prime Gauß period of type $(n_2, \pi_{r_t}(\mathcal{K}))$ over $\mathbb{F}_q$ with respect to ζ^{r/r_t}. The claim is proven.

Induction on the number t of prime divisors of r completes the proof of the lemma. □

5.1 Fast multiplication for decomposable Gauß periods

If a normal Gauß period is decomposable then its factorization into prime and prime power Gauß periods is related to a tower of fields. Each Gauß period along this tower satisfies the assumptions of Fact 3.6, i.e. the extension degrees are pairwise coprime.

PROPOSITION 5.4. *Let r, q, n, k be positive integers such that $q \ge 2$ and $r \ge 2$ are coprime and $\phi(r) = nk$. Let $r_1 \cdots r_t$ be the prime power decomposition of r. Let $\mathcal{K}$ be a subgroup of $\mathbb{Z}_r^\times$ of order k, set $\mathcal{K}_i = \pi_{r_i}(\mathcal{K})$ its image of order k_i onto $\mathbb{Z}_{r_i}^\times$ under the canonical projection π_{r_i}, and $n_i = \frac{\phi(r_i)}{k_i}$ for $1 \le i \le t$. Then the following are equivalent:*

(i) $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$ *and $\mathcal{K}$ is decomposable.*
(ii) $\langle q, \mathcal{K}_i\rangle = \mathbb{Z}_{r_i}^\times$ *for all $1 \le i \le t$, and $n = n_1 \cdots n_t$ with $n_1, \ldots, n_t$ pairwise coprime.*

PROOF. "(i)⇒(ii)" The canonical projection π_{r_i} is an epimorphism. Thus, $\mathbb{Z}_{r_i}^\times = \pi_{r_i}(\mathbb{Z}_r^\times) = \pi_{r_i}(\langle q, \mathcal{K}\rangle) = \langle q, \mathcal{K}_i\rangle$ for all $1 \le i \le t$. Since $\mathcal{K}$ is decomposable, we have $k = k_1 \cdots k_t$ and $n = \frac{\phi(r)}{k} = \prod_{1\le i\le t} \frac{\phi(r_i)}{k_i} = \prod_{1\le i\le t} n_i$. We prove by induction on the number of prime divisors that $n_1, \ldots, n_t$ are pairwise coprime. For $i = 1$ there is nothing to show. Thus, we suppose that the claim is true for $\mathcal{K}' = \mathcal{K}_1 \times \cdots \times \mathcal{K}_i$ which is a decomposable subgroup of $\mathbb{Z}_{r'}^\times$ of order k' where $r' = r_1 \cdots r_i$. By construction we have $\langle q, \mathcal{K}'\rangle = \mathbb{Z}_{r'}^\times$ and $n' = \frac{\phi(r')}{k'} = n_1 \cdots n_i$. We suppose that $d = \gcd(n', n_{i+1}) > 1$, i.e. $n' \cdot \frac{n_{i+1}}{d} < n_1 \cdots n_{i+1}$. Since $q^{n_{i+1}} \in \mathcal{K}_{i+1}$, we have $q^{n_{i+1}\cdot n'/d} \in \mathcal{K}_{i+1}$. But also $q^{n'\cdot n_{i+1}/d} \in \mathcal{K}'$ since $q^{n'} \in \mathcal{K}'$, and we conclude with the help of the Chinese Remainder Theorem that $q^{n'\cdot n_{i+1}/d} \in \mathcal{K}' \times \mathcal{K}_{i+1}$. Then $\#\langle q, \mathcal{K}' \times \mathcal{K}_{i+1}\rangle \le \frac{n'\cdot n_{i+1}}{d} \cdot k' \cdot k_{i+1} < (n' \cdot k') \cdot (n_{i+1} \cdot k_{i+1}) =$

$\phi(r')\cdot\phi(r_{i+1}) = \#(\mathbb{Z}_{r_1}^\times \times \cdots \times \mathbb{Z}_{r_{i+1}}^\times)$ which is a contradiction. Hence, n' and n_{i+1} are coprime. The induction hypothesis guarantees that $n_1, \ldots, n_i$ are pairwise coprime, and the claim holds for $n_1, \ldots, n_{i+1}$.
"(ii)⇒(i)" The group $\mathcal{K}$ can be regarded as a subgroup of $\mathcal{K}_1 \times \cdots \times \mathcal{K}_t$; hence k is a divisor of $k_1 \cdots k_t$. By assumption we have $n = n_1 \cdots n_t$. Thus, $k = \frac{\phi(r)}{n} = \prod_{1\le i\le t} \frac{\phi(r_i)}{n_i} = k_1 \cdots k_t$, i.e. the subgroup $\mathcal{K}$ is decomposable. We always have $\langle q, \mathcal{K}\rangle \subseteq \mathbb{Z}_r^\times$, and it remains to prove the other inclusion to show equality. Let a be an element in $\mathbb{Z}_r^\times$ and $a_i = \pi_{r_i}(a)$ for all $1 \le i \le t$. For $1 \le i \le t$ there are $c_i' \in \mathcal{K}_i$ and $0 \le h_i < n_i$ such that $a_i = q^{h_i} c_i' \in \langle q, \mathcal{K}_i\rangle = \mathbb{Z}_{r_i}^\times$. But $n_1, \ldots, n_t$ are pairwise coprime, and by the Chinese Remainder Theorem there exist $0 \le h < n$ with $h \equiv h_i \bmod n_i$ for $1 \le i \le t$. Since $q^{n_i} \in \mathcal{K}_i$, we have $q^h \equiv q^{h_i} c_i'' \bmod r_i$ for suitable $c_i'' \in \mathcal{K}_i$, $1 \le i \le t$. We set $c = (c_1'/c_1'', \ldots, c_t'/c_t'') \in \mathcal{K}$ to get $a \equiv q^h c \bmod r$. Thus $\langle q, \mathcal{K}\rangle \supseteq \mathbb{Z}_r^\times$ and hence $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$, as claimed. □

The factorization of a normal decomposable Gauß period α offers a recursive approach to do multiplication fast whenever $\mathbb{F}_{q^n}$ is represented by a normal basis $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n-1}})$.

Remark 5.5. *Let n_1 and n_2 be two coprime integers, and set $n = n_1 \cdot n_2$. Let $\alpha_1 \in \mathbb{F}_{q^{n_1}}$ and $\alpha_2 \in \mathbb{F}_{q^{n_2}}$ be normal elements over $\mathbb{F}_q$, and $\alpha = \alpha_1 \cdot \alpha_2$ be a normal element in $\mathbb{F}_{q^n}$.*

(i) The element α_2 is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^{n_1}}$.
(ii) Transforming an element given as linear combination of the conjugates of α over $\mathbb{F}_q$ into a linear combination of the conjugates of α_2 over $\mathbb{F}_{q^{n_1}}$ can be computed without operations in $\mathbb{F}_q$.

Proof. (i) This is just Lemma 3.9(ii).
(ii) Let $A = \sum_{0\le h<n} A_h \alpha^{q^h}$ be an element in $\mathbb{F}_{q^n}$. Let $h_i \equiv h \bmod n_i$ for $i = 1, 2$. Then $\alpha^{q^h} = \alpha_1^{q^{h_1}} \cdot \alpha_2^{q^{h_2}}$ and

$$A = \sum_{0\le h<n_1 n_2} A_h \left(\alpha_1^{q^{h_1}} \cdot \alpha_2^{q^{h_2}}\right) = \sum_{0\le h_2<n_2} \left(\sum_{0\le h_1<n_1} A_{(h_1,h_2)} \alpha_1^{q^{h_1}}\right) \alpha_2^{q^{h_2}}$$

where we identify h and $(h_1, h_2) = (h \bmod n_1, h \bmod n_2)$. Since n_1 and n_2 are coprime, we have $\{n_1 a \operatorname{rem} n_2 \colon 0 \le a < n_2\} = \{0 \le a < n_2\}$ and

$$A = \sum_{0\le h_2<n_2} \left(\sum_{0\le h_1<n_1} A_{(h_1,n_1 h_2)} \alpha_1^{q^{h_1}}\right) \alpha_2^{(q^{n_1})^{h_2}}.$$

This just means sorting the coefficients of A and can be done without operations in $\mathbb{F}_q$. □

5.1.1 A constructive proof.

We are now ready to apply fast polynomial multiplication if $\mathbb{F}_{q^n}$ is represented by a normal basis $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n-1}})$ over $\mathbb{F}_q$, where α is a decomposable Gauß period.

THEOREM 5.6. *Let α be a decomposable normal Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ with $\mathcal{K}$ a subgroup of $\mathbb{Z}_r^\times$, and let $r_1 \cdots r_t$ be the prime power decomposition of r. Then two elements in $\mathbb{F}_{q^n}$ given as linear combinations of the elements of the normal basis $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n-1}})$ can be multiplied with at most*

$$O(r \cdot \prod_{1 \le i \le t} (\log r_i \cdot \operatorname{loglog} r_i))$$

operations in $\mathbb{F}_q$.

PROOF. We prove the claim by induction on the number t of prime divisors of r. If $t = 1$, the claim follows from Theorem 4.26. Now we suppose $t \ge 2$. We can write $\alpha = \prod_{1 \le i \le t} \alpha_i^{q^{h_i}}$ as a product of conjugates of normal prime and prime power Gauß periods α_i of type $(n_i, \pi_{r_i}(\mathcal{K}))$ over $\mathbb{F}_q$ by Lemma 5.3. Set $n' = \frac{n}{n_t}$. The element $\alpha' = \prod_{1 \le i \le t-1} \alpha_i^{q^{h_i}}$ is normal in $\mathbb{F}_{q^{n'}}$ over $\mathbb{F}_q$. Since α is decomposable, Proposition 5.4 claims that n' and n_t are coprime. Then α_t is a normal prime or prime power Gauß period in $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^{n'}}$ by Remark 5.5(i). As claimed in Remark 5.5(ii), we can multiply two elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ by multiplying them in $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^{n'}}$. By Theorem 4.26, the multiplication can be done with at most $O(\mathsf{M}(r_t))$ operations (additions, multiplications) in $\mathbb{F}_{q^{n'}}$. Moreover, α' is a decomposable normal Gauß period of type $(n', \pi_{r_1}(\mathcal{K}) \times \cdots \times \pi_{r_{t-1}}(\mathcal{K}))$ over $\mathbb{F}_q$. By the induction hypothesis, multiplication in $\mathbb{F}_{q^{n'}}$ can be done with at most $O(\prod_{1 \le i \le t-1} \mathsf{M}(r_i))$ operations in $\mathbb{F}_q$, and the claim follows. □

EXAMPLE 2.5 CONTINUED. (iii) The decomposable Gauß period $\alpha = \zeta^{14} + \zeta^{24} + \zeta^4 + \zeta^{39}$ of type $(12, \{1, 26\})$ with $\{1, 26\} \subset \mathbb{Z}_{45}^\times$ over $\mathbb{F}_2$ is normal in $\mathbb{F}_{2^{12}}$. We calculate the product $\alpha^{2^2} \cdot \alpha$.

(i) As shown above, α factors into $\alpha = \alpha_5 \cdot \alpha_9$ with α_5 a prime Gauß period of type $(4, 1)$ over $\mathbb{F}_2$, and α_9 a prime power Gauß period of type $(3, \{1, 8\})$ over $\mathbb{F}_2$ where $\{1, 8\} \subset \mathbb{Z}_9^\times$. We transform the task into a multiplication over $\mathbb{F}_8$:

$$\alpha^4 \cdot \alpha = (\alpha_5^4 \cdot \alpha_9^4) \cdot (\alpha_5 \cdot \alpha_9) = (\alpha_5^4 \cdot \alpha_5) \cdot (\alpha_9^4 \cdot \alpha_9).$$

Now $\alpha_9^4 \cdot \alpha_9 = \alpha_9^2 + \alpha_9^4$ as computed in Example 4.2.

(ii) It remains to perform the arithmetic in $\mathbb{F}_8$ over $\mathbb{F}_2$. Since α_5 is a prime Gauß period, we have

$$\alpha_5^4 \cdot \alpha_5 = (\zeta^9)^4 \cdot (\zeta^9) = (\zeta^9)^5 = 1 = \alpha_5 + \alpha_5^2 + \alpha_5^4 + \alpha_5^8.$$

(iii) Combining both results gives

$$\begin{aligned}\alpha^4 \cdot \alpha &= (\alpha_5 + \alpha_5^2 + \alpha_5^4 + \alpha_5^8) \cdot (\alpha_9^2 + \alpha_9^4) \\ &= \alpha_5^{2^0}\alpha_9^{2^1} + \alpha_5^{2^1}\alpha_9^{2^1} + \alpha_5^{2^2}\alpha_9^{2^1} + \alpha_5^{2^3}\alpha_9^{2^1} + \alpha_5^{2^0}\alpha_9^{2^2} + \alpha_5^{2^1}\alpha_9^{2^2} \\ &\quad + \alpha_5^{2^2}\alpha_9^{2^2} + \alpha_5^{2^3}\alpha_9^{2^2} \\ &= \alpha^{2^4} + \alpha^{2^1} + \alpha^{2^{10}} + \alpha^{2^7} + \alpha^{2^8} + \alpha^{2^5} + \alpha^{2^2} + \alpha^{2^{11}},\end{aligned}$$

since $\alpha^{2^h} = \alpha_5^{2^{h_1}} \cdot \alpha_9^{2^{h_2}} = (\alpha_5 \cdot \alpha_9)^{2^{9h_1+4h_2}}$. ◊

6 From general to decomposable Gauß periods

There is one step missing to derive Theorem 2.7 from Theorem 5.6: Not every normal Gauß period is decomposable, as already illustrated in Example 2.5(iii).We now show that a normal Gauß period always entails a decomposable normal Gauß period with the same parameters. The proof of Theorem 6.3 is based on the following result of Gao (2001), Theorem 1.1.

FACT 6.1. *Let $\mathcal{Z}$ be an Abelian group of finite order. Let $\mathcal{Q}$ be a subset and $\mathcal{K}$ be a subgroup of $\mathcal{Z}$ such that $\mathcal{Z} = \langle \mathcal{Q}, \mathcal{K} \rangle$. Then, for any direct sum of $\mathcal{Z} = \mathcal{Z}_1 \times \cdots \times \mathcal{Z}_t$, there exists a subgroup $\mathcal{L}$ of the form $\mathcal{L} = \mathcal{L}_1 \times \cdots \times \mathcal{L}_t$ with $\mathcal{L}_i$ a subgroup of $\mathcal{Z}_i$ for $1 \le i \le t$ such that $\mathcal{Z} = \langle \mathcal{Q}, \mathcal{L} \rangle$ and $\mathcal{Z}/\mathcal{L} \cong \mathcal{Z}/\mathcal{K}$.*

For our situation, we formulate the following special case.

COROLLARY 6.2. *Let r and q be coprime positive integers greater than 2, and $r_1 \cdots r_t$ be the prime power factorization (2.2) of r. If there is a subgroup $\mathcal{K}$ of $\mathbb{Z}_r^\times$ with $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$, then there is a decomposable subgroup $\mathcal{L}$ of $\mathbb{Z}_r^\times$ of the same order $\#\mathcal{L} = \#\mathcal{K}$ such that $\langle q, \mathcal{L} \rangle = \mathbb{Z}_r^\times$.*

THEOREM 6.3. *Let r, q, n, k be positive integers with $r, q \ge 2$ such that r and q are coprime and $\phi(r) = nk$. Then there is a normal Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ with $\mathcal{K}$ a subgroup of $\mathbb{Z}_r^\times$ of order k if and only if such a period exists with decomposable $\mathcal{K}$.*

PROOF. This follows from Corollary 6.2 and the Normal Gauß period theorem 2.6. □

We merge Theorem 6.3 with Theorem 5.6, and apply fast polynomial multiplication to prove Theorem 2.7.

PROOF (of Theorem 2.7). Let α' be a general Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ generating a normal basis in $\mathbb{F}_{q^n}$. By Theorem 6.3 there is a normal

decomposable Gauß period α of type $(n, \mathcal{L})$ in $\mathbb{F}_{q^n}$ with $\#\mathcal{L} = \#\mathcal{K}$. Thus, we can write an element of $\mathbb{F}_{q^n}$ as a linear combination of the elements of the normal basis $\mathcal{N} = (\alpha, \ldots, \alpha^{q^{n-1}})$ over $\mathbb{F}_q$. In this case Theorem 5.6 states that we can apply fast polynomial multiplication to compute the product of two elements in $\mathbb{F}_{q^n}$. Inserting $\mathsf{M}(r_i) = O(r_i \log r_i \cdot \operatorname{loglog} r_i)$ for $1 \leq i \leq t$ proves the claimed bound on the number of operations in $\mathbb{F}_q$. □

In the final estimate of the theorem, one can replace the factor $\log(nk)$ by the entropy of $(r_1, \cdots, r_t)$.

7 Existence of normal Gauß periods

7.1 A criterion for the existence of a normal Gauß period

Given a prime power q and an integer n, how can we find normal Gauß periods in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$? We start with two previous results.

Fact 7.1 (Gao 2001, Theorem 1.4). *Let p be a prime, n and e be positive integers, and set $q = p^e$. There exist a positive integer r and a subgroup $\mathcal{K} \subseteq \mathbb{Z}_r^\times$ such that the Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ is normal in $\mathbb{F}_{q^n}$ if and only if the following hold:*

$$\gcd(e, n) = 1, \text{ and } 8 \not| n \text{ in the case } p = 2.$$

Fact 7.2 (Gao *et al.* 2000, Theorem 3.1). *Let $r = p^e$ be a prime power not divisible by 8, and let q be an integer greater than 1 and coprime to r. Let n be a positive divisor of $\phi(r)$, and $\mathcal{K}$ the uniquely determined subgroup of $\mathbb{Z}_r^\times$ of order $k = \frac{\phi(r)}{n}$. Then $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$ if and only if $\gcd(\frac{\phi(r)}{N}, n) = 1$, where $N = \operatorname{ord}_r(q)$ is the order of q in $\mathbb{Z}_r^\times$.*

For the non-cyclic group $\mathbb{Z}_{2^e}^\times$ with $e \geq 3$ this criterion is no longer true.

Example 7.3. For $r = 8$ and $\mathcal{K} = \{1, 7\}$, we have $\langle 3, \mathcal{K}\rangle = \{1, 3, 5, 7\} = \mathbb{Z}_8^\times$ and $\frac{\phi(8)}{\#\mathcal{K}} = \frac{4}{2} = 2$. Furthermore, $N = \operatorname{ord}_8(3) = 2$, so that $\frac{\phi(8)}{N} = 2$, and $\gcd\left(\frac{\phi(8)}{N}, \frac{\phi(8)}{\#\mathcal{K}}\right) = \gcd(2, 2) = 2 \neq 1$. ◊

For $n = 1$ and $k = \#\mathbb{Z}_{2^e}^\times$, we can always choose the trivial subgroup $\mathcal{K} = \mathbb{Z}_{2^e}^\times$ to get $\langle q, \mathcal{K}\rangle = \mathbb{Z}_{2^e}^\times$. For $n \geq 2$ we recall that $\mathbb{Z}_{2^e}^\times$ is the direct product of the two cyclic groups $\{\pm 1\} = \langle -1 \bmod 2^e\rangle$ and $\mathcal{Z}_{2^e} = \langle 5 \bmod 2^e\rangle = \{(4i + 1) \bmod 2^e : 0 \leq i < 2^{e-2}\}$. We start with the assumption that the subgroup generated by q has maximal possible order $N = \operatorname{ord}_{2^e}(q)$.

PROPOSITION 7.4. *Let $r \geq 16$ be a power of 2, and let $q \geq 3$ be odd. If $N = \operatorname{ord}_r(q) = 2^{e-2}$ and $n \geq 2$ is a divisor of N, then $\mathcal{K} = \{\pm 1\} \cdot \langle 5^n \bmod 2^e \rangle$ is a subgroup of $\mathbb{Z}_r^\times$ of order $k = \phi(r)/n$ such that $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$.*

PROOF. For $r = 2^e$ and $e \geq 4$, the subgroup $\mathcal{K}$ of $\mathbb{Z}_r^\times$ has order $2 \cdot \frac{2^{e-2}}{n} = \frac{2^{e-1}}{n} = \frac{\phi(r)}{n}$. We have $\#\langle q \rangle = N = 2^{e-2}$, by assumption. Thus, $\langle q \rangle / \{\pm 1\} = \mathcal{Z}_{2^e}$ because q generates a cyclic subgroup. By construction, $-1 \in \mathcal{K}$, hence $\langle q \rangle \cup (-1) \cdot \langle q \rangle$ is a subset of $\langle q, \mathcal{K} \rangle$ of order $2 \cdot 2^{e-2}$. We conclude that $\#\langle q, \mathcal{K} \rangle = \phi(r)$, and $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$, as claimed. □

LEMMA 7.5. *Let $e \geq 4$ be an integer, let q be an odd prime power and $\mathcal{K}$ be a subgroup of order k of $\mathbb{Z}_{2^e}^\times$ such that $\langle q, \mathcal{K} \rangle = \mathbb{Z}_{2^e}^\times$, and $n = \frac{\phi(2^e)}{k}$. If $n \geq 4$, then $\langle q \rangle$ has maximal order $N = \operatorname{ord}_{2^e}(q) = 2^{e-2}$.*

PROOF. Since n divides N, we have $N \geq 4$. Furthermore, the subgroup $\mathcal{K}$ has order $\#\mathcal{K} = \frac{\phi(2^e)}{n} \leq \frac{2^{e-1}}{4} = 2^{e-3} \geq 2$. Let $\bar{\cdot}\colon \mathbb{Z}_{2^e}^\times \to \mathcal{Z}_{2^e}$ be the canonical projection with $a = \bar{a} \cdot \{\pm 1\}$. Then $\langle \bar{q} \rangle$ is a cyclic subgroup of $\mathcal{Z}_{2^e}$ of order $N \geq 4$. The projection is an epimorphism. Hence, $\langle \bar{q}, \bar{\mathcal{K}} \rangle = \mathcal{Z}_{2^e}$. But $n' = \#\mathcal{Z}_{2^e} / \#\bar{\mathcal{K}} \geq 2^{e-2}/2^{e-3} = 2$ is divisible by 2, and the subgroup $\langle \bar{q} \rangle$ contains a subgroup of maximal order 2^{e-2}, since $\mathcal{Z}_{2^e}$ is cyclic. We conclude that $\langle \bar{q} \rangle = \mathcal{Z}_{2^e}$, and $N = \operatorname{ord}_{2^e}(q) \geq \#\mathcal{Z}_{2^e} = 2^{e-2}$. But a cyclic subgroup of $\mathbb{Z}_{2^e}^\times$ has order at most 2^{e-2} and thus $N = 2^{e-2}$. □

For $e = 3$, we have always $N = 2$, and there is a subgroup $\mathcal{K} \subseteq \mathbb{Z}_8^\times$ of order 2 with $\langle q, \mathcal{K} \rangle = \mathbb{Z}_8^\times$; for given $q \geq 3$ we can choose $\mathcal{K} = \langle a \rangle$ with $a \in \mathbb{Z}_8^\times \setminus \{1, q \bmod 8\}$.

The only case left is $n = 2$ and $2 \leq N < 2^{e-2}$ for $e \geq 4$. Here two different cases of q are important. Since we have q an odd prime power, either $q \equiv 1 \bmod 4$ or $q \equiv 3 \bmod 4$. These two cases have different projections of $\langle q \rangle$ onto $\{\pm 1\}$. We consider the canonical projection $\pi\colon \mathbb{Z}_{2^e}^\times \to \mathbb{Z}_4^\times$. Then $\ker \pi = \mathcal{Z}_{2^e}$, and we have a bijection between $\{\pm 1\} = \mathbb{Z}_{2^e}^\times / \ker \pi = \mathbb{Z}_{2^e}^\times / \mathcal{Z}_{2^e}$ and $\mathbb{Z}_4^\times$ applying the fundamental theorem on groups. Thus, $\langle q \rangle / \mathcal{Z}_{2^e}$ is $\{\pm 1\}$ if $q \equiv 3 \bmod 4$ and is $\{1\}$ if $q \equiv 1 \bmod 4$.

LEMMA 7.6. *Let $e \geq 4$ be an integer, $r = 2^e$, and let $q \geq 3$ be an odd integer with $2 \leq N = \operatorname{ord}_r(q) < 2^{e-2}$. Then there is a subgroup $\mathcal{K} \subseteq \mathbb{Z}_{2^e}^\times$ of order k such that $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$ if and only if $q \equiv 3 \bmod 4$.*

PROOF. For $q \equiv 3 \bmod 4$, we have $\langle q \rangle / \mathcal{Z}_{2^e} = \{\pm 1\}$. Since $n = 2 = \#\{\pm 1\}$ and $\{\pm 1\} \subseteq \langle q \rangle$ by assumption, we have $\langle q^{N/n} \rangle = \{\pm 1\}$. Choosing the subgroup $\mathcal{K} = \mathcal{Z}_{2^e}$ of order $k = 2^{e-2}$ gives $\langle q, \mathcal{K} \rangle = \mathbb{Z}_{2^e}^\times$.

For $q \equiv 1 \bmod 4$, we have $\langle q^{N/n} \rangle = \langle 5^{2^{e-3}} \bmod 2^e \rangle = \{5^{2^{e-3}}, 1\} \subset \mathbb{Z}_{2^e}^\times$. Since $e \geq 4$, there are three subgroups of $\mathbb{Z}_{2^e}^\times$ of order $k = 2^{e-2} \geq 4$ in this case:

$\mathcal{K}_1 = \langle 5 \bmod 2^e \rangle$, $\mathcal{K}_2 = \langle -5 \bmod 2^e \rangle$, and $\mathcal{K}_3 = \{\pm 1\} \cdot \langle 5^2 \bmod 2^e \rangle$. For $e \geq 4$, we have $2^{e-3} \geq 2$ and $5^{2^{e-3}} = (-5)^{2^{e-3}} = (5^2)^{2^{e-4}} \bmod 2^e$ is an element of all three subgroups. Hence, $\langle q, \mathcal{K}_i \rangle = \mathcal{K}_i \neq \mathbb{Z}_{2^e}^\times$ for $1 \leq i \leq 3$. Thus, there is no suitable subgroup in the case $q \equiv 1 \bmod 4$. □

We collect the findings above to get the following criteria on the existence of a suitable subgroup $\mathcal{K}$ in $\mathbb{Z}_{2^e}^\times$.

LEMMA 7.7. *Let $r \geq 8$ be a power of two. Let $q > 1$ be an odd integer, and n be a divisor of $N = \mathrm{ord}_r(q)$. Set $k = \phi(r)/n$. Then the following are equivalent:*

(i) There is a subgroup $\mathcal{K} \subseteq \mathbb{Z}_r^\times$ of order k with $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$.
(ii) One of the following criteria holds:
- *$n = 1$, or*
- *$n = 2$ and $q \equiv 3 \bmod 4$, or*
- *$N = r/4$.*

PROOF. We write $r = 2^e$ with $e \geq 2$. If one of the criteria in (ii) is satisfied then either $n = 1$ and $\mathcal{K} = \mathbb{Z}_{2^e}^\times$, or Proposition 7.4 or Lemma 7.6, respectively, guarantee the existence of a subgroup $\mathcal{K}$ of order k with $\langle q, \mathcal{K} \rangle = \mathbb{Z}_{2^e}^\times$ for $e \geq 4$. There are two more cases to consider. For $e = 3$ and $n = 2$ we have $N = \mathrm{ord}_8(q) = 2$. Then we can choose $\mathcal{K} = \{1, 3\}$ if $q \equiv 1 \bmod 4$ and $\mathcal{K} = \{1, 5\}$ if $q \equiv 3 \bmod 4$. Thus, it remains to prove that in the case $n = 2$ and $q \equiv 1 \bmod 4$ and $N < 2^{e-2}$ there is no suitable subgroup. We have $\langle q \rangle / \{\pm 1\} \subset \mathcal{Z}_{2^e}$, and thus $\langle q \rangle \subseteq \langle 5^2 \bmod 2^e \rangle$. But $5^2 \bmod 2^e$ is an element in all three subgroups of order $k = 2^{e-2}$ of $\mathbb{Z}_{2^e}^\times$; we have $5^2 \in \langle 5 \bmod 2^e \rangle$ and $5^2 = (-5)^2 \in \langle -5 \bmod 2^e \rangle$ and $1 \cdot 5^2 \in \{\pm 1\} \cdot \langle 5^2 \bmod 2^e \rangle$. Since we have discussed all possible cases, equivalence holds. □

We now have the following criterion for existence of a normal Gauß period. For squarefree r, this follows from Theorem 1.5 in Gao (2001).

THEOREM 7.8. *Let q be a prime power and r and n be positive integers such that $\gcd(r, q) = 1$ and n divides $\phi(r)$. Let $k = \frac{\phi(r)}{n}$ and $r_1 \cdots r_t$ be the prime power decomposition of r. Then the following properties are equivalent:*

(i) There is a subgroup $\mathcal{K}$ of $\mathbb{Z}_r^\times$ of order k such that the Gauß period α of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ is normal.
(ii) There are pairwise coprime positive integers $n_1, \ldots, n_t$ such that $n = n_1 \cdots n_t$, and
- *$\gcd(\frac{\phi(r_i)}{N_i}, n_i) = 1$ if r_i is not divisible by 8, and*
- *n_i divides N_i and either $n_i = 1$, or $n_i = 2$ and $q \equiv 3 \bmod 4$, or $N_i = 2^{e-2}$ if 8 divides r_i*

where $N_i = \mathrm{ord}_{r_i}(q)$ for $1 \leq i \leq t$.

PROOF. "(i)⇒(ii)" By Theorem 6.3 there is a decomposable Gauß period of type $(n, \mathcal{L})$ over $\mathbb{F}_q$ with $\langle q, \mathcal{L}\rangle = \mathbb{Z}_r^\times$. By Proposition 5.4 the $n_i = \frac{\phi(r_i)}{\#\pi_{r_i}(\mathcal{L})}$ for $1 \le i \le t$ are pairwise coprime and $n_1 \cdots n_t = n$. Furthermore, $\langle q, \pi_{r_i}(\mathcal{L})\rangle = \mathbb{Z}_{r_i}^\times$ and the criteria follows immediately with Fact 7.2 and Lemma 7.7.

"(ii)⇒(i)" By Fact 7.2 and Lemma 7.7, respectively, there is a subgroup $\mathcal{L}_i$ of order $k_i = \frac{\phi(r_i)}{n_i}$ such that $\langle q, \mathcal{L}_i\rangle = \mathbb{Z}_{r_i}^\times$ for all $1 \le i \le t$. Obviously, $\mathcal{L} = \mathcal{L}_1 \times \cdots \times \mathcal{L}_t$ meets the assumptions of Proposition 5.4. By the Normal Gauß period theorem 2.6, the criterion $\langle q, \mathcal{L}\rangle = \mathbb{Z}_r^\times$ is sufficient for the Gauß period of type $(n, \mathcal{L})$ over $\mathbb{F}_q$ to be normal. □

7.1.1 Experiments.

Tables 7.1 and 7.2 present results about the smallest values of k that lead to normal Gauß periods. Table 7.1 illustrates the progress made by the various categories of Gauß periods, going from the most specialized category "prime" in the first row to the general periods in the fourth row. In each row we find the percentage of n having a normal Gauß period of its row category with a smaller value of k than any the more specialized categories above it. The extension degree n goes from 2 to 10 000. The second column says, for example, that for 26.19% of those n some squarefree Gauß period in $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ has a smaller value of k than any prime Gauß period and that no general Gauß period improves on this k, and for 2.66% a general Gauß period provides a smaller k than any of the specialized categories in the three rows above. Similarly, Table 7.2 shows the percentage of extensions with squarefree Gauß periods when the value of k is bounded in terms of n, again for $2 \le n \le 10\,000$. For both tables, the value of r was limited to 10^6.

Acknowledgements

We thank the anonymous referees for a large number of corrections and useful suggestions, and Victor Pan for his efforts in handling the paper.

References

G. B. AGNEW, R. C. MULLIN & S. A. VANSTONE (1993). An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$. *IEEE Journal on Selected Areas in Communications* **11**(5), 804–813.

D.W. ASH, I.F. BLAKE & S.A. VANSTONE (1989). Low complexity normal bases. *Discrete Applied Mathematics* **25**, 191–210.

Minimal value of the parameter k for normal Gauß periods with respect to the class								
class \ q	2	3	5	7	11	13	17	19
prime	57.79	63.04	63.25	63.24	64.71	65.27	64.93	65.20
squarefree	26.19	29.22	30.35	23.35	25.78	25.16	32.33	22.59
prime power	0.87	0.89	0.92	0.84	0.95	1.08	0.79	0.62
general	2.66	6.85	5.48	12.56	8.56	8.49	1.95	11.58
no normal GP	12.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table 7.1
The percentage for which the minimal parameter $k \in \mathbb{N}_{\geq 1}$ is given by the special class of a Gauß period. The values are given for all field extensions $\mathbb{F}_{q^n}$ with $2 \leq n < 10000$. The values for q are given in the first row; e.g. the distribution over the binary field $\mathbb{F}_2$ is listed in the second column. The search for $k = \phi(r)/n$ is restricted to $r \leq 1\,000\,000$.

Existence of normal bases generated by a squarefree Gauß period with given parameter $k \geq 1$								
k \ q	2	3	5	7	11	13	17	19
$k = 1$	4.70	4.76	4.92	4.65	4.43	4.57	4.50	4.72
$k \leq 2$	25.22	25.78	24.60	23.21	23.77	22.67	25.18	22.75
$k \leq \log_2 n$	75.90	86.23	86.11	85.18	85.24	84.51	86.31	83.84
$k \leq \sqrt{n}$	87.24	99.65	99.68	99.63	99.66	99.57	99.57	99.50
$k < \infty$	87.50	100.00	100.00	100.00	100.00	100.00	100.00	99.98

Table 7.2
Percentage of field extensions $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with $2 \leq n < 10000$ for which there is a normal basis given by a squarefree Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$. The rows show the distribution if the value for $k = \#\mathcal{K}$ is restricted. We limited our experiments for r with $\phi(r) = nk$ to $2 \leq r < 1\,000\,000$.

Ian F. Blake, Ron M. Roth & Gadiel Seroussi (1998). Efficient Arithmetic in $GF(2^n)$ through Palindromic Representation. Technical Report HPL-98-134, Visual Computing Department, Hewlett Packard Laboratories. Available via `www.hpl.hp.com/techreports/98/HPL-98-134.html`.

David G. Cantor (1989). On Arithmetical Algorithms over Finite Fields. *Journal of Combinatorial Theory, Series A* **50**, 285–300.

Sandra Feisel, Joachim von zur Gathen & M. Amin Shokrollahi (1999). Normal bases via general Gauß periods. *Mathematics of Computation* **68**(225), 271–290. URL `http://www.ams.org/journal-getitem?pii=S0025-5718-99-00988-6`.

Shuhong Gao (2001). Abelian Groups, Gauss Periods, and Normal Bases. *Finite*

Fields and Their Applications **7**(1), 148–164.
Shuhong Gao, Joachim von zur Gathen & Daniel Panario (1995). Gauss periods and fast exponentiation in finite fields. In *Proceedings of LATIN '95,* Valparaíso, Chile, number 911 in Lecture Notes in Computer Science, 311–322. Springer-Verlag. ISSN 0302-9743. Final version in Mathematics of Computation and Journal of Symbolic Computation.
Shuhong Gao, Joachim von zur Gathen & Daniel Panario (1998). Gauss periods: orders and cryptographical applications. *Mathematics of Computation* **67**(221), 343–352. URL `http://www.ams.org/jourcgi/amsjournal?fn=120&pg1=pii&s1=S0025%571898009351`. With microfiche supplement.
Shuhong Gao, Joachim von zur Gathen, Daniel Panario & Victor Shoup (2000). Algorithms for Exponentiation in Finite Fields. *Journal of Symbolic Computation* **29**(6), 879–889. URL `http://www.idealibrary.com/links/doi/10.1006/jsco.1999.0309`.
Carl Friedrich Gauss (1801). *Disquisitiones Arithmeticae.* Gerh. Fleischer Iun., Leipzig. English translation by Arthur A. Clarke, Springer-Verlag, New York, 1986.
Dirk Hachenberger (1997). *Finite Fields: Normal Bases and Completely Free Elements.* The Kluwer international series in engineering and computer science. Kluwer Academic Publishers, Boston/Dordrecht/London.
D. Jungnickel (1993). *Finite Fields: Structure and Arithmetics.* BI Wissenschaftsverlag, Mannheim.
Rudolf Lidl & Harald Niederreiter (1983). *Finite Fields.* Number 20 in Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading MA.
Alfred J. Menezes, Ian F. Blake, XuHong Gao, Ronald C. Mullin, Scott A. Vanstone & Tomik Yaghoobian (1993). *Applications of finite fields.* Kluwer Academic Publishers, Norwell MA.
R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone & R. M. Wilson (1989). Optimal normal bases in GF(p^n). *Discrete Applied Mathematics* **22**, 149–161.
A. Schönhage (1977). Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica* **7**, 395–398.
A. Schönhage & V. Strassen (1971). Schnelle Multiplikation großer Zahlen. *Computing* **7**, 281–292.
Alfred Wassermann (1993). Zur Arithmetik in endlichen Körpern. *Bayreuther Math. Schriften* **44**, 147–251.