INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

FACTORING CYCLOTOMIC POLYNOMIALS OVER FINITE FIELDS

By

Gregory C. Stein

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

1997

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

Apr. 17, 1997 — Alphonse Thomas Vasquez
Date — Chair of Examining Committee

Apr. 17, 1997 — Isaac Chavel (ATV)
Date — Executive Officer

Alphonse Vasquez

Carlos Moreno

Martin Moskowitz

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Factoring Cyclotomic Polynomials over Finite Fields

by

Gregory C. Stein

Advisor: Professor Alphonse Vasquez

We examine the problem of deterministically factoring the r^{th} cyclotomic polynomial, $\Phi_r(x)$, over $\mathbb{F}_p$, where r and p are distinct primes, by looking at the traces of the roots of $\Phi_r(x)$ over $\mathbb{F}_p$.

Chapter 1 is an introduction and a brief review of the theory of cyclotomy. In Chapter 2 we show how to derive the factors of $\Phi_r(x)$ using the traces of the roots of $\Phi_r(x)$ over $\mathbb{F}_p$. We then demonstrate a deterministic algorithm for finding these factors in time polynomial in r and $\log p$ in the case where $\Phi_r(x)$ has precisely two irreducible factors over $\mathbb{F}_p$. In Chapter 3 we construct an algebraic model to further explore the results of Chapter 2 and describe a technique for constructing an $\mathbb{F}_p$-algebra isomorphic to the Berlekamp sub-algebra of $\mathbb{F}_p/\Phi_r(x)$. In Chapter 4 we use some techniques of linear algebra to derive explicit matrix descriptions of some of the maps discussed in Chapter 3. We further use these techniques to reduce our problem to that of factoring polynomials which split over $\mathbb{F}_p$.

Acknowledgments

I would like to thank the City University of New York, for being flexible enough to allow me to finish my doctorate while working full-time, as well as my advisor, Professor Al Vasquez, whose insights and patience were invaluable, and Professors Moreno and Moskowitz for their time and suggestions. I would also like to thank Professor Mel Hochster of the University of Michigan for getting me interested in algebra in the first place.

Most importantly, I thank all of my friends and family for their patience and support. I would especially like to thank my sister and my niece, Jennie and Rebecca, for their love and understanding, my buddy Neil Ostrander for his diversion and friendship, Dana Cazzulino and Maria Oquendo for their lovely dinners, Molly Welch and the state of Vermont for a quiet place to get away, and Adeline Goldminc for our conversations.

Contents

Chapter 1

Introduction and review

1.1 Introduction

This thesis was originally motivated by a desire to explore the possibility of deterministically constructing arbitrary extensions of finite fields which involved as little arbitrary choice as possible. For this reason we choose to look at techniques which will work 'quickly' over finite fields with very large characteristic, techniques which will depend only upon the degree of the extension and the cost of performing arithmetic operations in the base field. In so much as constructing an extension of degree m over $\mathbb{F}_{p^d}$, p prime, is the same as constructing an extension of degree md over $\mathbb{F}_p$, we shall focus on extensions of prime fields.

In 1990, V. Shoup [SHO] showed that the problem of deterministically constructing

finite fields of order p^r can be reduced to that of factoring cyclotomic polynomials of prime degree over prime fields. We therefore concern ourselves here with the problem of factoring cyclotomic polynomials over prime fields. The case where these two primes are the same is covered very effectively by Artin-Schreier theory[1] , so we will only be concerned with the case where the primes are distinct. We will be most interested in the case where $p \gg r$ and in finding techniques which will run in time polynomial in r and $\log p$.

We will be interested in deterministic methods which will be fast, even over very large finite fields, and will often wish to analyze how quickly our techniques work. In this text the term *operations* refers to an addition or multiplication over the base field. By $O(a)$ operations we mean that the number of operations is bounded by some fixed multiple of a. By $a^{O(1)}$ operations we mean that the number of operations is bounded by some fixed polynomial in a.

Please note that many extremely fast probabilistic algorithms exist for factoring cyclotomic polynomials over finite fields and the techniques presented here are not intended to compete with these techniques in running time. For this reason, analyses of running times is not as efficient as possible. For more precise running times for various operations the reader is referred to [BIN].

[1] See, for example, [LAN], p.325, Theorem 6.4 or [SHO] Lemma 2.3.

1.2 A Review of Cyclotomy

Throughout this text we shall apply the results of the theory of cyclotomy to explore the relationship between the traces of the r^{th} roots of unity and the factors of the irreducible factors of the r^{th} cyclotomic polynomial over finite fields. To this end we begin with a brief review of the theory of cyclotomy. This information can be found in either Storer [STO], Dickson [DIC], or Myerson [MYE].

In the classical treatment of cyclotomy the following definitions and observations are made over $\mathbb{Q}$. Given a prime number, r, positive integers d and m, so that $dm = r-1$, and a primitive element α of $\mathbb{F}_r$, that is an element of $\mathbb{F}_r$ which generates $\mathbb{F}_r^*$, we define the *cyclotomy classes*

$$\begin{aligned} H_0 &= \{1, \alpha^m, \alpha^{2m}, \cdots, \alpha^{(d-1)m}\} \\ H_1 &= \{\alpha, \alpha^{m+1}, \alpha^{2m+1}, \cdots, \alpha^{(d-1)m+1}\} \\ &\vdots \\ H_i &= \{\alpha^i, \alpha^{m+i}, \alpha^{2m+i}, \cdots, \alpha^{(d-1)m+i}\} \\ &\vdots \\ H_{m-1} &= \{\alpha^{m-1}, \alpha^{m+(m-1)}, \alpha^{2m+(m-1)}, \cdots, \alpha^{(d-1)m+(m-1)}\}. \end{aligned} \tag{1.1}$$

Note that H_0 is the unique subgroup of $\mathbb{F}_r^*$ of order d and that the $H_i = \alpha^i H_0$ are the cosets of H_0 in $\mathbb{F}_r^*$. Noting that $\alpha^{m+i}H_0 = \alpha^i H_0$, we see that we may index the H_i with $\mathbb{Z}/m\mathbb{Z}$. If we were to use a primitive element other than α we would

get precisely the same cyclotomy classes, though perhaps in a different order. Most generally we could forget about α altogether and simply define H_0 to be the unique subgroup of $\mathbb{F}_r^*$ with order d and then, for each $a \in \mathbb{F}_r^*$, define $H_a = aH$ to be the coset in $\mathbb{F}_r^*/H_0$ with coset representative a. It will be convenient, however, to be able to index these cosets with $\mathbb{Z}/m\mathbb{Z}$ and remember that changing our choice of α permutes the indexing of the H_i.

Given α, we can set up the H_i and then we define the *cyclotomic numbers*, $(i,j)_\alpha$, $i,j \in \mathbb{Z}/m\mathbb{Z}$, to be the number of solutions to

$$x + 1 = y$$

for $x \in H_i$, $y \in H_j$. That is, if we set $H_i^+ = \{x + 1 \mid x \in H_i\} \subseteq \mathbb{F}_r$, then $(i,j)_\alpha = \#(H_i^+ \cap H_j)$. It should be noted that if $H_1', \cdots, H_{m-1}'$ is the ordering of the cosets that we get by choosing a different primitive element, α', then, if $H_{i_1} = H_{i_2}'$ and $H_{j_1} = H_{j_2}'$, we have $(i_1, j_1)_\alpha = (i_2, j_2)_{\alpha'}$. As it will generally be assumed that a specific primitive element has been chosen we shall usually supress the subscript on the cyclotomic numbers.

An important point to make at this point is that one may find primitive elements of $\mathbb{F}_r^*$ by trial and error in time $r^{O(1)}$ (for each $b \in \mathbb{F}_r^*$ simply check whether $b^{\frac{r-1}{2}} = -1$, roughly $\log \frac{r-1}{2}$ multiplications in $\mathbb{F}_r$ at most r times), that H_i can be computed by performing d multiplications in $\mathbb{F}_r$, that H_i^+ can be computed by performing $d < r$ additions in $\mathbb{F}_r$, that $H_i^+ \cap H_j$ can be found by doing d^2 comparisons in $\mathbb{F}_r$, and then

(i,j) can be computed by counting to at most d. Therefore all of the cyclotomy classes and cyclotomic numbers can be deterministically computed in time $r^{O(1)}$.

If we now think of working over some field, $\mathbb{F}$, and let ζ represent a primitive r^{th} root of unity in an appropriate extension field, $\mathbb{K}$, then one defines the *periods*, t_i, by

$$t_i = \sum_{j=0}^{d-1} \zeta^{\alpha^{mj+i}} = \sum_{a \in H_i} \zeta^a. \tag{1.2}$$

Noting that $t_i = t_{m+i}$ we may consider the t_i to be indexed by $\mathbb{Z}/m\mathbb{Z}$.

Although the classical theory of cyclotomy is used to study roots of unity over the rationals, all of the basic definitions and theorems make sense and are true over any field. In particular, we wish to look at a special application of this theory and some of its results over the finite field $\mathbb{F}_p$ with the intention of factoring the r^{th} cyclotomic polynomial, $\Phi_r = \frac{x^r-1}{x-1} = 1 + x + x^2 + \cdots + x^{r-1}$, over $\mathbb{F}_p$, r and p distinct primes. The elementary theory of finite fields[2] tells us that in this case Φ_r will factor into m distinct irreducible polynomials, each of degree d, where d =ord(p,r), the order of p in $\mathbb{F}_r^*$, that is, the least integer so that $p^d \equiv 1 \bmod r$, and $m = \frac{r-1}{d}$. We now compute the cyclotomy classes using this choice of d and m.

As H_0 is the unique subgroup of $\mathbb{F}_r^*$ with order d, and ord$(p,r) = d$, it follows that

$$H_0 = < p > = \{1, p, p^2, \cdots, p^{d-1}\} \subseteq \mathbb{F}_r^*. \tag{1.3}$$

Now, it is true that there will be a primitive element, α, of $\mathbb{F}_r^*$ with the property that $\alpha^m = p$ and, using this α we can generate $H_1, \cdots, H_{m-1}$ as described in the classical

[2] See, for example [LID1] or [LID2].

approach. It will be more convenient, however, to make a more canonical choice. To this end, we shall agree to choose α to be the primitive element of $\mathbb{F}_r^*$ with the least positive residue and set $H_i = \alpha^i H_0$, $i \in \mathbb{Z}/m\mathbb{Z}$. One advantage of this canonical choice of α is that if the primes p_1 and p_2 have the same order mod r, as for instance will be the case when $p_1 \equiv p_2 \bmod r$, then the cyclotomy classes and the cyclotomic numbers will not only be the same, but will have the same indexing.

Now let ζ be a primitive r^{th} root of unity in some extension field of $\mathbb{F}_p$, say $\mathbb{F}_{p^d}$, the splitting field of $\Phi_r(x)$ over $\mathbb{F}_p$, then the irreducible factors of $\Phi_r(x)$ over $\mathbb{F}_p$ are

$$g_i(x) = \prod_{j=0}^{d-1}(x - \zeta^{\alpha^i p^j}) = \prod_{a \in H_i}(x - \zeta^a), i \in \mathbb{Z}/m\mathbb{Z} \tag{1.4}$$

and note that in this context the periods

$$t_i = \sum_{j=0}^{d-1} \zeta^{\alpha^i p^j} = \sum_{a \in H_i} \zeta^a, i \in \mathbb{Z}/m\mathbb{Z} \tag{1.5}$$

have the property that $t_i = \text{trace}_{\mathbb{F}_p}(g_i(x))$, by which we mean that t_i is the sum of the roots of $g_i(x)$ or, equivalently, that $t_i = \text{trace}_{\mathbb{F}_p}(\zeta^{\alpha^i})$ or, equivalently, that $-t_i$ is the coefficient of x^{d-1} in $g_i(x)$.

Of interest in Chapter 3 is the product formula, relating the periods and the cyclotomic numbers, that can be found as a corollary to Lemma 8 on p. 39 of [STO] which gives an explicit formula for the product of any two periods as a $\mathbb{Z}$-linear combination of the periods by

$$t_i t_{i+k} = \left(\sum_{h=0}^{m-1}(k,h)t_{i+h}\right) + d\theta_k \tag{1.6}$$

where (k,h) is the cyclotomic number discussed on p.4 and where

$$\theta_k = \begin{cases} 1, \text{ if } d \text{ is even and } k = 0 \\ 1, \text{ if } d \text{ is odd and } k = m/2 \\ 0 \text{ otherwise} \end{cases} \cdot \tag{1.7}$$

Note that in our case the fact that $t_0 + \cdots + t_{m-1} = -1$ allows us to rewrite (1.6) as

$$t_i t_{i+k} = \sum_{h=0}^{m-1} [(k,h) - d\theta_k]\, t_{i+h} \tag{1.8}$$

which, by replacing k by $j-i$, becomes

$$\begin{aligned} t_i t_j &= t_i t_{i+(j-i)} \\ &= \sum_{h=0}^{m-1} [(j-i,h) - d\theta_{j-i}]\, t_{i+h} \\ &= \sum_{h=0}^{m-1} [(j-i,h-i) - d\theta_{j-i}]\, t_h. \end{aligned} \tag{1.9}$$

It will also be of use to include here some of the basic identities concerning the cyclotomic numbers. All of the following are proved in Lemma 3 on p. 25 of [STO].

Lemma 1 *1.* $(i,j) = (m-i, j-i)$

2. $(i,j) = \begin{cases} (j,i) & d \text{ even} \\ \left(j+\frac{m}{2}, i+\frac{m}{2}\right) & d \text{ odd} \end{cases}$

3. $\sum_{j=0}^{m-1}(i,j) = d - \theta_i$ *where* $\theta_i = \begin{cases} 1 & d \text{ even}, i = 0 \\ 1 & d \text{ odd}, i = \frac{m}{2} \\ 0 & \text{otherwise} \end{cases}$

4. $\sum_{i=0}^{m-1}(i,j) = d - \eta_j$ *where* $\eta_j = \begin{cases} 1 & j = 0 \\ 0 & \text{otherwise} \end{cases}$

A simple observation we will need later on, but not proved in any of the citations above, is the following lemma.

Lemma 2 *For $d \neq 1$, in $\mathbb{F}_r$*

$$\sum_{\gamma \in H_i} \gamma = 0.$$

Proof: Note that, in $\mathbb{F}_r$

$$\sum_{\gamma \in H_i} \gamma = \alpha^i + \alpha^i p + \alpha^i p^2 + \cdots + \alpha^i p^{d-2} + \alpha^i p^{d-1} \tag{1.10}$$

and so

$$p \sum_{\gamma \in H_i} \gamma = \alpha^i p + \alpha^i p^2 + \alpha^i p^3 + \cdots + \alpha^i p^{d-1} + \alpha^i p^d \tag{1.11}$$

and, since $p^d = 1$, we have

$$p \sum_{\gamma \in H_i} \gamma = \sum_{\gamma \in H_i} \gamma. \tag{1.12}$$

But $d \neq 1 \Rightarrow p \neq 1$ and p and r distinct primes so $p \neq 0$. Hence $\sum_{\gamma \in H_i} \gamma = 0$. ■

Chapter 2

The coefficients of the factors of the cyclotomic polynomial

In this chapter we shall explore the relationship between the traces of the irreducible factors of cyclotomic polynomials and the coefficients of these factors. We shall reduce the problem of deterministically factoring the r^{th} cyclotomic polynomial over $\mathbb{F}_p$, p and r distinct primes, in time $r^{O(1)}$, to that of finding the traces of the r^{th} roots of unity over $\mathbb{F}_p$. We shall use these results to make some observations about the irreducible factors of the cyclotomic polynomial.

2.1 Preliminary definitions

In what follows let r and p be distinct primes, $d = \text{ord}(p, r)$, $m = \frac{r-1}{d}$, and let α be a primitive element of $\mathbb{Z}/r\mathbb{Z}$. For $i \in \mathbb{Z}/m\mathbb{Z}$, define

$$H_i = \{\alpha^i, \alpha^i p, \cdots, \alpha^i p^{d-1}\} = \alpha^i H_0 \subseteq \mathbb{Z}/r\mathbb{Z}, \tag{2.1}$$

set $\Phi_r(x) = 1 + x + \cdots + x^{r-1} \in \mathbb{F}_p[x]$, the r^{th} cyclotomic polynomial, and let ζ be a primitive r^{th} root of unity in $\mathbb{F}_{p^d}$. For $i \in \mathbb{Z}/m\mathbb{Z}$ we define

$$g_i(x) = \prod_{k=0}^{d-1}(x - \zeta^{\alpha^i p^k}) \in \mathbb{F}_p[x] \tag{2.2}$$

and note that these are the irreducible factors of $\Phi_r(x)$ over $\mathbb{F}_p$. For $i \in \mathbb{Z}/m\mathbb{Z}$ define

$$t_i = \sum_{k=0}^{d-1} \zeta^{\alpha^i p^k}, \tag{2.3}$$

the trace of $g_i(x)$ over $\mathbb{F}_p$.

2.2 A combinatorial result

In this section we show that we may compute, in time $r^{O(1)}$, each of the coefficients of the $g_i(x)$ in a specific way as $\mathbb{Z}$-linear combinations of the t_i without knowing, *a priori*, the arithmetic structure of $\mathbb{F}_{p^d}$, the factorization of $\Phi_r(x)$ over $\mathbb{F}_p$, or the values of the t_i as elements of $\mathbb{F}_p$. To accomplish this we first make a combinatorial observation.

Given p and r, distinct primes, let α be a primitive element of $\mathbb{Z}/r\mathbb{Z}$ and let d, m and the H_i be as defined as in the previous section. Rather than work in $\mathbb{F}_{p^d}$, we shall work in $\mathcal{R}$, where $\mathcal{R} = \mathbb{Z}[Y]/(Y^r - 1)$. In $\mathcal{R}$ define the counterpart of t_i to be

$$v_i = \sum_{k=0}^{d-1} Y^{\alpha^i p^k}, i \in \mathbb{Z}/m\mathbb{Z} \tag{2.4}$$

and the counterpart of $g_i(x)$ to be

$$f_i(x) = \prod_{k=0}^{d-1}(x - Y^{\alpha^i p^k}), i \in \mathbb{Z}/m\mathbb{Z} \tag{2.5}$$

in $\mathcal{R}[x]$.

Lemma 3 *There exist unique integers,* $\left\{\alpha_{st}^{(u)}\right\}_{\substack{u,t\in\mathbb{Z}/m\mathbb{Z}\\ s\in\mathbb{Z}/d\mathbb{Z}}}$ *and* $\left\{\beta_s^{(u)}\right\}_{\substack{u\in\mathbb{Z}/m\mathbb{Z}\\ s\in\mathbb{Z}/d\mathbb{Z}}}$, *which can be computed deterministically in time* $r^{O(1)}$ *so that the coefficient of* x^s *in* $f_u(x)$ *is*

$$(-1)^{d-s}\left(\beta_s^{(u)}+\sum_{i=0}^{m-1}\alpha_{si}^{(u)}v_i\right). \tag{2.6}$$

We postpone the proof until we have made some observations.

Note that, as $Y^r=1$ in $\mathcal{R}$, we may view the exponents of Y as elements of $\mathbb{Z}/r\mathbb{Z}$. Therefore each $f_u\in\mathcal{R}$ has a unique coset representative which is a polynomial in x of degree d whose coefficients are $(r-1)^{st}$ degree polynomials in Y over $\mathbb{Z}$.

Let $\mathcal{S}$ be the collection of all cardinality l subsets of $\mathbb{Z}/d\mathbb{Z}$. Expanding (2.5) formally, we can write the coefficient of x^{d-l} in $f_u(x)$ as

$$(-1)^l\sum_{\{i_1,\cdots,i_l\}\in\mathcal{S}}Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} \tag{2.7}$$

and note that there is a one-to-one correspondence with the $\binom{d}{l}$ summands in (2.7) with the elements of $\mathcal{S}$. We define an equivalence relation on $\mathcal{S}$ by

$$\{i_1,\cdots,i_l\}\sim\{i_1+k,\cdots,i_l+k\},k\in\mathbb{Z}/d\mathbb{Z} \tag{2.8}$$

and note that under this relation no partition contains more than d elements. Now let $\mathcal{S}_1\subseteq\mathcal{S}$ be the union of all partitions containing precisely d elements of $\mathcal{S}$ and let $\mathcal{S}_2\subseteq\mathcal{S}$ be the union of all partitions containing fewer than d elements of $\mathcal{S}$. In addition, let

$$\mathcal{T}_1 = \{\{i_1, \cdots, i_l\} \in \mathcal{S}_1 \mid p^{i_1} + \cdots + p^{i_l} \equiv 0 \bmod d\} \tag{2.9}$$

$$\mathcal{T}_2 = \mathcal{S}_1 - \mathcal{T}_1$$

and we now observe that if $p^{i_1} + \cdots + p^{i_l} \equiv 0 \bmod r$, then $p^{i_1+k} + \cdots + p^{i_l+k} = p^k(p^{i_1} + \cdots + p^{i_l}) \equiv 0 \bmod r$ and conversely, since $p^k \not\equiv 0 \bmod r$, and r is prime. That is, if $\{i_1, \cdots, i_l\} \backsim \{j_1, \cdots, j_l\}$ then $\{i_1, \cdots, i_l\} \in \mathcal{T}_1$ (or $\mathcal{T}_2$) if, and only if, $\{j_1, \cdots, j_l\} \in \mathcal{T}_1$ (or $\mathcal{T}_2$, respectively). Therefore we may write $\mathcal{T}_1 = P_1 \cup \cdots \cup P_{n_1}$ and $\mathcal{T}_2 = Q_1 \cup \cdots \cup Q_{n_2}$, disjoint unions, where the P_i and the Q_i are partitions under the equivalence relation. Further note that $\mathcal{S} = \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{S}_2$ where $\mathcal{T}_1$, $\mathcal{T}_2$ and $\mathcal{S}_2$ are pairwise disjoint. We may now rewrite (2.7) as

$$(-1)^l \left(\sum_{k=1}^{n_1} \sum_{\{i_1, \cdots i_l\} \in P_k} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} + \sum_{k=1}^{n_2} \sum_{\{i_1, \cdots i_l\} \in Q_k} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} + \sum_{\{j_1, \cdots, j_l\} \in \mathcal{S}_2} Y^{\alpha^u(p^{j_1} + \cdots + p^{j_l})} \right). \tag{2.10}$$

Lemma 4 *P_k, Q_k and $\mathcal{S}_2$ as above, then*

1. Σ_1. $\sum_{\{i_1, \cdots i_l\} \in P_k} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = d$.
2. Σ_2. $\sum_{\{i_1, \cdots i_l\} \in Q_k} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = v_s$, *where* $p^{i_1} + \cdots + p^{i_l} \in H_{s-u}$
3. Σ_3. $\sum_{\{j_1, \cdots j_l\} \in \mathcal{S}_2} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = \#(\mathcal{S}_2)$.

Proof of 1): $\{i_1, \cdots i_l\} \in P_k \Rightarrow p^{i_1} + \cdots + p^{i_l} \equiv 0 \bmod r \Rightarrow Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = 1$. Since $\#(P_k) = d$, it follows that

$$\sum_{\{i_1, \cdots i_l\} \in P_k} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = \sum_{\{i_1, \cdots i_l\} \in P_k} 1 = \#(P_k) = d. \tag{2.11}$$

Proof of 2): Say

$$Q_k = \{\{i_1, \cdots, i_l\}, \cdots, \{i_1 + (d-1), \cdots, i_l + (d-1)\}\} \tag{2.12}$$

then $\{i_1, \cdots, i_l\} \in Q_k \Rightarrow p^{i_1} + \cdots + p^{i_l} \neq 0 \in \mathbb{F}_r \Rightarrow \alpha^u(p^{j_1} + \cdots + p^{j_l}) \neq 0 \in \mathbb{F}_r$. Therefore there exists e_k, $1 \leq e_k \leq m-1$, so that $p^{i_1} + \cdots + p^{i_l} = \alpha^{e_k} p^l \in H_{e_k}$, hence $p^{i_1+n} + \cdots + p^{i_l+n} = \alpha^{e_k} p^{n+l} \in H_{e_k}$ so

$$\sum_{\{i_1, \cdots i_l\} \in Q_k} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = \sum_{n=0}^{d-1} Y^{\alpha^{u+e_k} p^{n+l}} = \sum_{n=0}^{d-1} Y^{\alpha^{u+e_k} p^n} = v_{u+e_k}. \tag{2.13}$$

Proof of 3): If $\{j_1, \cdots, j_l\} \in \mathcal{S}_2$ then there exists $n \in \mathbb{Z}/d\mathbb{Z} - \{0\}$ so that $\{j_1, \cdots, j_l\} = \{j_1 + n, \cdots, j_l + n\} \in \mathcal{S}_2$, hence $p^{j_1} + \cdots + p^{j_l} = (p^{j_1} + \cdots + p^{j_l})\, p^n \in \mathbb{F}_r$, but $p^n \not\equiv 1$ or $0 \bmod r$, so $p^{j_1} + \cdots + p^{j_l} \equiv 0 \bmod r$, hence $\alpha^u(p^{j_1} + \cdots + p^{j_l}) \equiv 0 \bmod r$, and therefore $Y^{\alpha^u(p^{j_1} + \cdots + p^{j_l})} = 1 \in R$ so

$$\sum_{\{j_1, \cdots j_l\} \in \mathcal{S}_2} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = \sum_{\{j_1, \cdots j_l\} \in \mathcal{S}_2} 1 = \#(S_2) \tag{2.14}$$

and the lemma is proved. ■

We are now in a position to prove Lemma 3

Proof of Lemma 3: If we now let $\alpha^{(u)}_{d-l,t}$ be the number of the $Q_1, \cdots, Q_{n_2}$ from Lemma 4 so that $\sum_{\{i_1, \cdots i_l\} \in Q_k} Y^{\alpha^u(p^{i_1} + \cdots + p^{i_l})} = v_t$ and let $\beta^{(u)}_{d-l}$ equal $\#(S_2) + dn_2$ then, referring to Lemma 4 and (2.10), we have that the coefficient of x^{d-l} in

$f_u(x)$ is

$$(-1)^l \left(\sum_{k=1}^{n_1} \sum_{\{i_1,\cdots i_l\}\in P_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{k=1}^{n_2} \sum_{\{i_1,\cdots i_l\}\in Q_k} Y^{\alpha^u(p^{i_1}+\cdots+p^{i_l})} + \sum_{\{j_1,\cdots,j_l\}\in \mathcal{S}_2} Y^{\alpha^u(p^{j_1}+\cdots+p^{j_l})} \right) \quad (2.15)$$

$$= (-1)^l \left(\sum_{k=1}^{n_1} d + \sum_{\{i_1,\cdots i_l\}\in Q_k} v_s + \#(\mathcal{S}_2) \right) = (-1)^l \left(\beta_{d-l}^{(u)} + \sum_{i=0}^{m-1} \alpha_{d-l,i}^{(u)} v_i \right)$$

where the s in the next to last expression is the s such that $p^{i_1}+\cdots+p^{i_l} \in H_{s-u}$.

To see that these integers are unique it suffices to note that $1, v_0, v_1, \cdots, v_{m-1}$ each have unique coset representatives in $\mathcal{R}$ that are polynomials in Y with coefficients in $\mathbb{Z}$ with degree no more than r, and that no two of these share terms of like degree, and therefore linearly independent in $\mathbb{Q}[Y]/(Y^r-1)$, viewed as an r-dimensional $\mathbb{Q}$ vector space, therefore unique in $\mathcal{R} = \mathbb{Z}[Y]/(Y^r-1)$, which can be thought of as sitting inside of $\mathbb{Q}[Y]/(Y^r-1)$.

All that remains is to show that these coefficients can be computed in time $r^{O(1)}$. Recalling from the paragraph following (2.6) that the $f_i(x)$ can be viewed as d^{th} degree polynomials in x whose coefficients are $(r-1)^{st}$ degree polynomials in Y, the results of Lemma 4 show that $\alpha_{st}^{(u)}$ is the coefficient for v_t in the coefficient for Y^u in the coefficient of x^s. We now demonstrate a technique for expanding (2.5). Note that this method differs from the one in Lemma 4.

Let

$$W_i^{(u)}(x) = \prod_{k=0}^{i} \left(x - Y^{\alpha^u p^k}\right) \in \mathcal{R}[x] \tag{2.16}$$

and note that $f_u(x) = W_{d-1}^{(u)}(x)$ and that

$$W_{i+1}^{(u)}(x) = W_i^{(u)}(x)\left(x - Y^{\alpha^u p^{i+1}}\right) = xW_i^{(u)}(x) - Y^{\alpha^u p^{i+1}} W_i^{(u)}(x). \tag{2.17}$$

For any $i \in \mathbb{Z}/d\mathbb{Z}$, $W_i^{(u)}(x)$ is a polynomial in x of degree at most $d < r$ with coefficients which are polynomials in Y of degree at most r. Note that the coefficients of these polynomials in Y are integers bounded above by the $\alpha_{st}^{(u)}$ which are in turn bounded by $\#(S) = \binom{d}{l} < 2^d$. Computing $W_{i+1}^{(u)}(x)$ from $W_i^{(u)}(x)$ as suggested in (2.17) we see that computing $xW_i^{(u)}(x)$ involves increasing each exponent of x in $W_i^{(u)}(x)$ by 1, $O(r)$ operations. We then compute $Y^{\alpha^u p^{i+1}} W_i^{(u)}(x)$ by multiplying each of the polynomial coefficients of $W_i^{(u)}(x)$ by $Y^{\alpha^u p^{i+1}}$ which involves at most $d \cdot r$ additions modulo r, or $O(r^2 \log r)$ operations. Finally, computing $xW_i^{(u)}(x) - Y^{\alpha^u p^{i+1}} W_i^{(u)}(x)$ involves at most $d \cdot r$ additions of integers bounded by 2^d, or $O(r^3)$ operations. As this process is repeated d times we see that an upper bound for the computation is $O(r^4)$ operations. This completes the proof of Lemma 3. ■

Before specializing to finite fields, we make the following observation concerning the cyclic behavior of the coefficients in the v_j expansion of the coefficients of the f_i.

Lemma 5 *For $i, t \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z}$, $\beta_s^{(i)} = \beta_s^{(0)}$ and $\alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)}$.*

Proof: Let $f_i(x) = \prod_{k=0}^{d-1}\left(x - Y^{\alpha^i p^k}\right) \in \mathcal{R}[x]$ as in (2.5). As in (2.10) we get that the coefficient of x^{d-l} in $f_i(x)$ is

$$(-1)\left(\sum_{k=1}^{n_1+n_2}\sum_{\{i_1,\cdots i_l\}\in P_k} Y^{\alpha^i p^{i_1}+\cdots+\alpha^i p^{i_l}} + \sum_{\{j_1,\cdots,j_l\}\in S_2} Y^{\alpha^i p^{j_1}+\cdots+\alpha^i p^{j_l}}\right) \tag{2.18}$$

where S_2 is as in Lemma 4 and here the P_k run through all of the partitions in S_1. Again, if $e_k \equiv p^{i_1} + \cdots + p^{i_l} \bmod r$ for some one of the $\{i_1, \cdots i_l\} \in P_k$ then we have

$$\sum_{\{i_1,\cdots i_l\}\in P_k} Y^{\alpha^i p^{i_1}+\cdots+\alpha^i p^{i_l}} = \sum_{u=0}^{d-1} Y^{e_k\alpha^i p^u} = \sum_{u=0}^{d-1} Y^{\alpha^u\left(p^{i_1+u}+\cdots+p^{i_l+u}\right)}. \tag{2.19}$$

If $e_k = 0 \in \mathbb{F}_r$ then (2.19) is precisely d. Otherwise, we have that

$$\{e_k\alpha^i, e_k\alpha^i p, \cdots, e_k\alpha^i p^{d-1}\} = H_{s+i} \tag{2.20}$$

where $e = \alpha^s p^i \in H_s$, some i, hence (2.19) is v_{s+i}. If $\{j_1, \cdots, j_l\} \in S_2$ then, as in Lemma 4, $\sum_{\{j_1,\cdots,j_l\}\in S_2} Y^{\alpha^i p^{j_1}+\cdots+\alpha^i p^{j_l}} = \#(S_2)$. So certainly $\beta_s^{(i)} = \beta_s^{(0)}$. Now, $\alpha_{s,t+i}^{(i)}$ is the number of partitions which yield v_{t+i} and these are the same partitions which yielded v_t in the coefficient of x^{d-l} for $f(x)$. So $\alpha_{s,t+i}^{(i)} = \alpha_{s,t}^{(0)}$, or $\alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)}$. ■

The following version of the preceding lemma will prove useful later on.

Corollary 1 *For i, t, $k \in \mathbb{Z}/m\mathbb{Z}, s \in \mathbb{Z}/d\mathbb{Z}$,*

$$\beta_s^{(i)} = \beta_s^{(k)},\ \alpha_{s,t-k}^{(i)} = \alpha_{s,t}^{(i+k)} \text{ and } \alpha_{s,t}^{(i)} = \alpha_{s,t+k}^{(i+k)}.$$

That is, if the coefficient of x^s is

$$\lambda_0 t_0 + \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_{m-2} t_{m-2} + \lambda_{m-1} t_{m-1} + \beta \text{ in } g_0 \tag{2.21}$$

then the coefficient of x^s *is*

$$\begin{array}{c} \lambda_{m-1}t_0 + \lambda_0 t_1 + \lambda_1 t_2 + \cdots + \lambda_{m-3}t_{m-2} + \lambda_{m-2}t_{m-1} + \beta \text{ in } g_1 \\ \lambda_{m-2}t_0 + \lambda_{m-1}t_1 + \lambda_0 t_2 + \cdots + \lambda_{m-4}t_{m-2} + \lambda_{m-3}t_{m-1} + \beta \text{ in } g_2 \\ \lambda_{m-3}t_0 + \lambda_{m-2}t_1 + \lambda_{m-1}t_2 + \cdots + \lambda_{m-5}t_{m-2} + \lambda_{m-4}t_{m-1} + \beta \text{ in } g_3 \\ \vdots \\ \lambda_1 t_0 + \lambda_2 t_1 + \lambda_2 t_2 + \cdots + \lambda_{m-1}t_{m-2} + \lambda_0 t_{m-1} + \beta \text{ in } g_{m-1}. \end{array} \tag{2.22}$$

Proof: That $\beta_s^{(i)} = \beta_s^{(k)}$ is immediate from Lemma 5. To see that $\alpha_{s,t-k}^{(i)} = \alpha_{s,t}^{(i+k)}$ simply observe that from Lemma 5 and using $t-k$ in place of t, we get $\alpha_{s,t-k}^{(i)} = \alpha_{s,t-i-k}^{(0)}$ and, by replacing i by $i+k$, $\alpha_{s,t}^{(i+k)} = \alpha_{s,t-i-k}^{(0)}$. To see that $\alpha_{s,t}^{(i)} = \alpha_{s,t+k}^{(i+k)}$ note that $\alpha_{s,t}^{(i)} = \alpha_{s,t-i}^{(0)} = \alpha_{s,t}^{(0)}$ and, by replacing i by $i+k$, and replacing t by $t+k$, $\alpha_{s,t+k}^{(i+k)} = \alpha_{s,t+k-(i+k)}^{(0)} = \alpha_{s,t-i}^{(0)}$. ■

We now wish to restate Lemma 3 for our situation. That is, working over $\mathbb{F}_p$ rather than $\mathcal{R}$.

Theorem 1 *There exist subsets of* $\mathbb{F}_p$, $\left\{\alpha_{st}^{(u)}\right\}_{\substack{u,t\in\mathbb{Z}/m\mathbb{Z} \\ s\in\mathbb{Z}/d\mathbb{Z}}}$ *and* $\left\{\beta_s^{(u)}\right\}_{\substack{u\in\mathbb{Z}/m\mathbb{Z} \\ s\in\mathbb{Z}/d\mathbb{Z}}}$, *which can be computed deterministically in time* $r^{O(1)}$, *so that the coefficient of* x^s *in* $g_u(x)$ *is*

$$(-1)^{d-s}\left(\beta_s^{(u)} + \sum_{i=0}^{m-1} \alpha_{si}^{(u)} t_i\right). \tag{2.23}$$

Furthermore, we have that for i, t, $k \in \mathbb{Z}/m\mathbb{Z}$, *and* $s \in \mathbb{Z}/d\mathbb{Z}$,

$$\begin{aligned} \beta_s^{(i)} &= \beta_s^{(0)} \\ \alpha_{s,t}^{(i)} &= \alpha_{s,t-i}^{(0)} \\ \beta_s^{(i)} &= \beta_s^{(k)} \\ \alpha_{s,t-k}^{(i)} &= \alpha_{s,t}^{(i+k)} \\ \alpha_{s,t}^{(i)} &= \alpha_{s,t+k}^{(i+k)}. \end{aligned}$$

Proof: To prove the existence and to compute the $\alpha_{st}^{(u)}$ and $\beta_s^{(u)}$ we simply reduce, mod p, those integers discussed in Lemma 3, Lemma 4 and Corollary 1. When replacing Y by ζ and computing over $\mathbb{F}_p$ we need only compute some of the additions modulo p, thereby replacing one factor of r in the time bound by a factor of $\log p$, thereby giving us a time bounded by a polynomial in r^3 and $\log p$. Please note that if $p \gg r$, in particular, if $p > 2^d$, then, since these coefficients never exceed 2^d, we may perform the additions as before without reduction modulo p. Hence, the number of operations needed to compute the $\alpha_{st}^{(u)}$ and $\beta_s^{(u)}$ is bounded by a fourth degree polynomial in r. ■

It should be noted that since $1 = -t_0 - t_1 - \cdots - t_{m-1}$ we may rewrite (2.23) as

$$(-1)^{d-s}\left[\sum_{i=0}^{m-1}\left(\alpha_{si}^{(u)} - \beta_s^{(u)}\right)t_i\right] \tag{2.24}$$

allowing us to write the coefficients of the $g_i(x)$ as homogeneous linear polynomials in the t_i. If we now define

$$\delta_{si}^{(u)} = \alpha_{si}^{(u)} - \beta_s^{(u)}, \tag{2.25}$$

then we see that the coefficient of x^s in $g_u(x)$ is

$$(-1)^{d-s}\left[\sum_{i=0}^{m-1}\delta_{si}^{(u)}t_i\right]. \tag{2.26}$$

We may further observe that, as a result of Lemma 5 and Corollary 1, we have, for i,

$t, k \in \mathbb{Z}/m\mathbb{Z}$ and $s \in \mathbb{Z}/d\mathbb{Z}$,

$$\begin{aligned} \delta_{st}^{(i)} &= \delta_{s,t-i}^{(0)} \\ \delta_{s,t-k}^{(i)} &= \delta_{s,t}^{(i+k)} \\ \delta_{s,t}^{(i)} &= \delta_{s,t+k}^{(i+k)}. \end{aligned} \tag{2.27}$$

Please note that in the statement of Theorem 1 we have lost the uniqueness portion of Lemma 3 and that, as $t_0 + \cdots + t_{m-1} = -1$, the $\alpha_{si}^{(u)}$ and $\beta_s^{(u)}$ will not be unique. However, we shall see in Chapter 4 that, subject to (2.26) and (2.27), the δ's are unique.

One remark that should be made at this point is that in the computation of the $\alpha_{si}^{(u)}$ and the $\beta_s^{(u)}$, p itself has only been used to determine the cyclotomy classes $H_0, \cdots, H_{m-1}$ in $\mathbb{Z}/r\mathbb{Z}$. Therefore, if p_1 and p_2 are primes with $\mathrm{ord}(p_1, r) = \mathrm{ord}(p_2, r)$, in particular, if $p_1 \equiv p_2 \bmod r$, they will generate the same cyclotomy classes and in the same order, assuming that the same primitive element, α, for F_r^* was used. Hence, aside from the reduction mod p_1 or p_2, the $\alpha_{si}^{(u)}$, $\beta_s^{(u)}$ and $\delta_{si}^{(u)}$ will be the same for both p_1 and p_2 and that, if both of these primes are $> 2^d$, we need not even concern ourselves about this reduction. It should also be remarked that replacing the primitive element, α, of $\mathbb{F}_r^*$ by any other primitive element will also generate the same cyclotomy classes, though possibly in a different order. That is, if p_1 and p_2 are primes with the property that $\mathrm{ord}(p_1, r) = \mathrm{ord}(p_2, r)$, then the cyclic subgroups

$< p_1 >$ and $< p_2 >$ of $\mathbb{F}_r^*$ are the same (since $\mathbb{F}_r^*$ has only one subgroup of order d) and will therefore have the same cosets as well. If we let $H_0 =< p_1 >=< p_2 >$ and let α be any primitive element of $\mathbb{F}_r^*$ and define $H_i = \alpha^i H_0$, then we may duplicate the results of Theorem 1 and find identical representations of the irreducible factors of $\Phi_r(x)$ over $\mathbb{F}_{p_1}$ and $\mathbb{F}_{p_2}$.

Example Let $p = 31$ and $r = 19$. We find that $d = 6$, $m = 3$, choose $\alpha = 2$ and let ζ represent a primitive 19^{th} root of unity over $\mathbb{F}_{31}$. From this we compute the cyclotomy classes

$$\begin{aligned} H_0 &= \{1, 12, 11, 18, 7, 8\} \\ H_1 &= \{2, 5, 3, 17, 14, 16\} \\ H_2 &= \{4, 10, 6, 15, 9, 13\} \end{aligned}$$

and the cyclotomy periods

$$\begin{aligned} t_0 &= \zeta + \zeta^{12} + \zeta^{11} + \zeta^{18} + \zeta^7 + \zeta^8 \\ t_1 &= \zeta^2 + \zeta^5 + \zeta^3 + \zeta^{17} + \zeta^{14} + \zeta^{16} \\ t_2 &= \zeta^4 + \zeta^{10} + \zeta^6 + \zeta^{15} + \zeta^9 + \zeta^{13}. \end{aligned}$$

Using the techniqes from Lemma 3 we arrive at the following table that describes the coefficients of the powers of ζ for each power of x. The number in row x^s and the column ζ^i is $\alpha_{si}^{(0)}$ and the number in column 1 and row x^s is $\beta_s^{(0)}$.

		H_0						H_1						H_2					
	1	ζ	ζ^{12}	ζ^{11}	ζ^{18}	ζ^{7}	ζ^{8}	ζ^{2}	ζ^{5}	ζ^{3}	ζ^{17}	ζ^{14}	ζ^{16}	ζ^{4}	ζ^{10}	ζ^{6}	ζ^{15}	ζ^{9}	ζ^{13}
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
x^2	3	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
x^3	2	2	2	2	2	2	2	1	1	1	1	1	1	0	0	0	0	0	0
x^4	3	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
x^5	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
x^6	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

hence

$$g_0 = x^6 - t_0x^5 + (3 + t_0 + t_2)x^4 - (2 + 2t_0 + t_1)x^3 + (3 + t_0 + t_2)x^2 - t_0x + 1$$

and by Lemma 5 we have

$$\begin{aligned} g_1 &= x^6 - t_1x^5 + (3 + t_1 + t_0)x^4 - (2 + t_1 + 2t_2)x^3 + (3 + t_1 + t_0)x^2 - t_1x + 1 \\ g_2 &= x^6 - t_2x^5 + (3 + t_2 + t_1)x^4 - (2 + t_2 + 2t_0)x^3 + (3 + t_2 + t_1)x^2 - t_2x + 1. \end{aligned}$$

Alternatively, using the characterization in (2.24), we get

$$\begin{aligned} g_0 &= x^6 - t_0x^5 - (2t_0 + 3t_1 + 2t_2)x^4 + (t_1 + 2t_2)x^3 - (2t_0 + 3t_1 + 2t_2)x^2 - t_0x + 1 \\ g_1 &= x^6 - t_1x^5 - (2t_0 + 2t_1 + 3t_2)x^4 + (2t_0 + t_2)x^3 - (2t_0 + 2t_1 + 3t_2)x^2 - t_1x + 1 \\ g_2 &= x^6 - t_2x^5 - (3t_0 + 2t_1 + 2t_2)x^4 + (t_0 + 2t_1)x^3 - (3t_0 + 2t_1 + 2t_2)x^2 - t_2x + 1. \end{aligned}$$

Recalling the remarks immediately preceding this example, we see that we may replace $p = 31$ with any prime, p, so that $\text{ord}(p, 19) = 6$, and we will get precisely the same results. ■

2.3 Further Results

An immediate consequence of Theorem 1 is that if we already know the traces of the irreducible factors of $\Phi_r(x)$ over $\mathbb{F}_p$, in the appropriate order, then we may determine these factors. However, if we simply know what the traces are, then, although we can arbitrarily denote any of these traces as t_0, there are $(m-1)!$ possible orders for the remaining ones. We shall see in Section 3.3 a technique which will allow us to compute the factors of the irreducible factors of $\Phi_r(x)$ in time $r^{O(1)}$ given the traces of the $g_i(x)$ and that, in many cases, knowing a single one of the traces will allow us to generate the others in the appropriate order in polynomial time. For now though, we may state some nice results which do not depend upon knowing any of the traces. The first[1] solves the problem of deterministically factoring $\Phi_r(x)$ in time $r^{O(1)}$ in the case where $m = 2$. We shall also see a technique for computing the sum of the $g_i(x)$ and some results on symmetries which occur among the coefficients of the $g_i(x)$.

[1] This result first appeared in [STE].

2.3.1 The Case $m = 2$

In this section we shall see, using the techniques from the previous sections, that we may deterministically compute the complete factorization of $\Phi_r(x)$ in time $(r \log p)^{O(1)}$ in the special case where $m = 2$. We shall also see some applications to constructing field extensions of $\mathbb{F}_p$.

Theorem 2 *Given p and r primes, with ord$(p, r) = \frac{r-1}{2}$, then we may factor $\Phi_r(x)$, the r^{th} cyclotomic polynomial, over $\mathbb{F}_p$ deterministically in time $(r \log p)^{O(1)}$.*

As a result of Theorem 1 it suffices to compute the traces t_0 and t_1. Note that if $p = 2$ then, since $t_0 + t_1 = -1$, we must have that, without loss of generality, $t_0 = 0$ and $t_1 = 1$. So assume $p \neq 2$ and consider the polynomial $(x - t_0)(x - t_1) = x^2 - (t_0 + t_1)x + t_0 t_1 = x^2 + x + t_0 t_1$. Hence

$$t_0, t_1 = \frac{-1 \pm \sqrt{1 - 4t_0 t_1}}{2}. \tag{2.28}$$

We first need to make the following observation.

Lemma 6 *p, r, t_0 and t_1 as in Theorem 2, then*

$$1 - 4t_0 t_1 = \begin{cases} r & r \equiv 1 \bmod 4 \\ -r & r \equiv 3 \bmod 4 \end{cases}. \tag{2.29}$$

Proof: From Lemma 8 on p.38 of [STO] we have that

$$t_0 t_1 = (1, 0)t_0 + (1, 1)t_1 + d\theta \tag{2.30}$$

where $(1, 0)$ and $(1, 1)$ are cyclotomic numbers and where

$$\theta = \begin{cases} 0 & \text{for } d \text{ even} \\ 1 & \text{for } d \text{ odd} \end{cases}.$$

If $r \equiv 1 \bmod 4$, then d is even, so $\theta = 0$ and, by Lemma 6 on p.30 of [STO], we have $(1,0) = (1,1) = \frac{d}{2} = \frac{r-1}{4}$, hence

$$1 - 4t_0t_1 = 1 - 4\left[\frac{r-1}{4}(t_0 + t_1)\right] = r. \tag{2.31}$$

If $r \equiv 3 \bmod 4$, then d is odd, hence $\theta = 1$, and, again by Lemma 6 on p.30 of [STO], we have $(1,0) = (1,1) = \frac{d-1}{2} = \frac{r-3}{4}$, hence

$$1 - 4t_0t_1 = 1 - 4\left[\frac{r-3}{4}(t_0 + t_1) + \frac{r-1}{2}\right] = 1 - 4\left(\frac{r+1}{4}\right) = -r.\blacksquare \tag{2.32}$$

R. Schoof recently showed [SCH] that if $\pm n$ are quadratic residues $\bmod p$ then $\sqrt{\pm n}$ can be deterministically computed in $\mathbb{F}_p$ in time $(|n| \log p)^{O(1)}$. Since t_0 and t_1 exist it follows that $\pm r$ are quadratic residues $\bmod p$ and so $\sqrt{\pm r}$ can be deterministically computed in time $(r \log p)^{O(1)}$. This completes the proof of Theorem 2.

Shoup showed [SHO] that if we may factor $\Phi_r(x)$ over $\mathbb{F}_p$, then we may deterministically construct an r^{th} degree extension field of $\mathbb{F}_p$ in time polynomial in r and $\log p$. Further, if the prime decomposition of n is $q_1^{e_1} \cdots q_k^{e_k}$, and we may construct extension fields of orders $q_1, \cdots, q_k$ then we can construct an extension field of order n deterministically in time polynomial in n and $\log p$. In the same paper Shoup shows how to construct extensions of degree 2. This, combined with Theorem 2, proves the following theorem.

Theorem 3 *If n is a positive integer with prime decomposition $2^e q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$, where $ord(p, q_i) = \frac{q_i - 1}{2}$, $i = 0, \cdots, k$, then we may deterministically construct an extension field of order n over $\mathbb{F}_p$, p prime, in time $n^{O(1)}$.*

2.3.2 The sum of the $g_i(x)$

In this section we see how to compute the sum of the irreducible factors of the cyclotomic polynomial.

We combine the results of Theorem 1 and Lemma 5 to prove

Lemma 7 *Given p and r, distinct primes, then we may explicitly compute $g_0(x) + \cdots + g_{m-1}(x) \in \mathbb{F}_p[x]$, the sum of the irreducible factors of the r^{th} cyclotomic polynomial, in time $r^{O(1)}$.*

Proof: Adding the coefficients for x^s from Theorem 1 we have

$$\sum_{u=0}^{m-1}\left(\beta_s^{(u)} + \sum_{i=0}^{m-1}\alpha_{s,i}^{(u)}t_i\right) = \sum_{u=0}^{m-1}\beta_s^{(u)} + \sum_{u=0}^{m-1}\left(\sum_{i=0}^{m-1}\alpha_{s,i}^{(u)}t_i\right) \tag{2.33}$$

now, using Lemma 5, we have that (2.33) equals

$$\begin{aligned}
m\beta_s^{(0)} + \sum_{u=0}^{m-1}\left(\sum_{i=0}^{m-1}\alpha_{s,i-u}^{(0)}t_i\right) &= m\beta_s^{(0)} + \sum_{i=0}^{m-1}\left(\sum_{u=0}^{m-1}\alpha_{s,i-u}^{(0)}t_i\right) = \\
m\beta_s^{(0)} + \sum_{i=0}^{m-1}\left[t_i\left(\sum_{u=0}^{m-1}\alpha_{s,i-u}^{(0)}\right)\right] &= m\beta_s^{(0)} + \sum_{i=0}^{m-1}\left[t_i\left(\sum_{a=0}^{m-1}\alpha_{s,a}^{(0)}\right)\right] = \\
m\beta_s^{(0)} + \left(\sum_{a=0}^{m-1}\alpha_{s,a}^{(0)}\right)\left(\sum_{i=0}^{m-1}t_i\right) &= m\beta_s^{(0)} - \left(\sum_{a=0}^{m-1}\alpha_{s,a}^{(0)}\right).
\end{aligned}$$

Theorem 1 proves that the $\alpha_{s,a}^{(0)}$ and $\beta_s^{(0)}$ may be computed in time $r^{O(1)}$.■

Example: From the example on p.20 we get that the sum of the factors of $\Phi_{19}(x)$ over $\mathbb{F}_p$ for any prime p with $\text{ord}(p, 19) = 6$ is

$$3x^6 - (t_0 + t_1 + t_2)x^5 + (-7t_0 - 7t_1 - 7t_2)x^4 - (-3t_0 - 3t_1 - 3t_2)x^3$$

$$+(-7t_0 - 7t_1 - 7t_2)x^2 - (t_0 + t_1 + t_2)x + 3$$

$$= 3x^6 + x^5 + 7x^4 - 3x^3 + 7x^2 + x + 3.\blacksquare$$

2.3.3 Some results on the coefficients of the $g_i(x)$

We now wish to demonstrate some symmetries which occur among the $\alpha_{st}^{(u)}$ and the $\beta_s^{(u)}$. We begin by comparing the coefficients of x^l and x^{d-l}.

Let $\mathcal{S}$ be the collection of all l element subsets of $\mathbb{Z}/d\mathbb{Z}$ and $\mathcal{S}'$ the collection of all $d-l$ element subsets of $\mathbb{Z}/d\mathbb{Z}$. Let $\varphi : \mathcal{S} \to \mathcal{S}'$ be the bijection $\varphi(I) = I^C$, the complement of I in $\mathbb{Z}/d\mathbb{Z}$. Define an equivalence relation, $\sim$, on both $\mathcal{S}$ and $\mathcal{S}'$ as in the proof of Lemma 3, that is, $\{i_1, \cdots, i_l\} \sim \{i_1 + k, \cdots, i_l + k\}$, $k \in \mathbb{Z}/m\mathbb{Z}$, and note that for $I_1, I_2 \in \mathcal{S}$ we have

$$I_1 \sim I_2 \Leftrightarrow \varphi(I_1) \sim \varphi(I_2). \tag{2.34}$$

Let $\mathcal{S}_1$ be the subset of $\mathcal{S}$ consisting of all elements belonging to equivalence classes with d elements and $\mathcal{S}_2$ the set of all elements of $\mathcal{S}$ belonging to equivalence classes with fewer than d elements. Similarly define $\mathcal{S}_1'$ and $\mathcal{S}_2'$, subsets of $\mathcal{S}'$. Let $P_1, \cdots, P_t$ and $P_1', \cdots, P_w'$ be the equivalence classes contained in $\mathcal{S}_1$ and $\mathcal{S}_1'$ respectively. By (2.34) we see that $\varphi(\mathcal{S}_1) = \mathcal{S}_1'$, and $\varphi(\mathcal{S}_2) = \mathcal{S}_2'$, that $w = t$, and that, with the appropriate ordering, $\varphi(P_k) = \varphi(P_k')$, $1 \leq k \leq t$. Recalling (2.18) we note that in

$f_i(x)$ the coefficient of x^{d-l} is

$$(-1)^l \left(\sum_{k=1}^{t} \sum_{\{i_1,\cdots,i_l\}\in P_k} Y^{\alpha^i\left(p^{i_1}+\cdots+p^{i_l}\right)} + \sum_{\{j_1,\cdots,j_l\}\in S_2} Y^{\alpha^i\left(p^{j_1}+\cdots+p^{j_l}\right)} \right) \tag{2.35}$$

and that the coefficient of x^l is

$$(-1)^{d-l} \left(\sum_{k=1}^{t} \sum_{\{i_{l+1},\cdots,i_d\}\in P'_k} Y^{\alpha^i\left(p^{i_{l+1}}+\cdots+p^{i_d}\right)} + \sum_{\{j_{l+1},\cdots,j_d\}\in S'_2} Y^{\alpha^i\left(p^{j_{l+1}}+\cdots+p^{j_d}\right)} \right). \tag{2.36}$$

Recall that $\alpha_{lt}^{(0)}$ is the number of P_k in (2.35) that yield v_t, that $\alpha_{d-l,t}^{(0)}$ is the number of P'_k in (2.36) that yield v_t and that $\beta_l^{(0)} = \#(S_2) + d$(the number of equivalence classes from (2.35) which do not yield any v_t) and that $\beta_{d-l}^{(0)} = \#(S'_2) + d$(the number of equivalence classes from (2.36) which do not yield any v_t).

Lemma 8 *d even, then, for $s \in \mathbb{Z}/d\mathbb{Z}$, $i, k \in \mathbb{Z}/m\mathbb{Z}$, we have*

$$\begin{aligned} \beta_l^{(i)} &= \beta_{d-l}^{(i)} \\ \alpha_{lk}^{(i)} &= \alpha_{d-l,k}^{(i)}. \end{aligned}$$

Proof: Note that $\left(p^{d/2}\right)^2 = 1 \in \mathbb{F}_r$. Since $\mathrm{ord}(p, r) = d$, it follows that $p^{d/2} \neq 1$, hence $p^{d/2} = -1 \in \mathbb{F}_r$. Now, if d is even, then $d/2 \in \{0, 1, \cdots, d\} \subset \mathbb{F}_r$. More generally, for $k = 0, \cdots, \frac{d}{2} - 1$, we have

$$\alpha^i p^k = -\alpha^i p^{d/2+k} \in \mathbb{F}_r. \tag{2.37}$$

That is, in $H_i = \{\alpha^i, \alpha^i p, \cdots, \alpha^i p^d\} \subseteq \mathbb{F}_r^*$ we have

$$\alpha^i = -\alpha^i p^{d/2}, \alpha^i p = -\alpha^i p^{d/2+1}, \cdots, \alpha^i p^{d/2-1} = -\alpha^i p^{d-1}. \tag{2.38}$$

Therefore

$$\gamma \in H_i \Leftrightarrow -\gamma \in H_i \tag{2.39}$$

and, recalling Lemma 2,

$$\sum_{\gamma \in H_i} \gamma = 0. \tag{2.40}$$

Let $I = \{i_1, \cdots, i_l\} \in S$ and $I^C = \{i_{l+1}, \cdots, i_d\} \in S'$. From (2.40) we have that, since $H_0 = \left\{p^0, p, p^2, \cdots, p^{d-1}\right\}$ and $\{i_1, \cdots, i_d\} = \{0, 1, \cdots, d-1\}$,

$$p^{i_1} + \cdots + p^{i_l} = -(p^{i_{l+1}} + \cdots + p^{i_d}) \in \mathbb{F}_r. \tag{2.41}$$

Now, if $I = \{i_1, \cdots, i_l\} \in S_2$, hence $I^C = \{i_{l+1}, \cdots, i_d\}$, and $p^{i_1} + \cdots + p^{i_l} = 0$, then $p^{i_{l+1}} + \cdots + p^{i_d} = 0$ so $Y^{p^{i_1}+\cdots+p^{i_l}} = Y^{p^{i_l+1}+\cdots+p^{i_d}} = 1 \in \mathcal{R}$, therefore

$$\sum_{\{i_1,\cdots,i_l\} \in S_2} Y^{p^{i_1}+\cdots+p^{i_l}} = \sum_{\{i_{l+1},\cdots,i_d\} \in S_2'} Y^{p^{i_l+1}+\cdots+p^{i_d}} = \#(S_2). \tag{2.42}$$

Similarly, if $\{i_1, \cdots, i_l\} \in P_k$ and $p^{i_1} + \cdots + p^{i_l} = 0 \in \mathbb{F}_r$, then

$$\sum_{\{i_1,\cdots,i_l\} \in P_k} Y^{p^{i_1}+\cdots+p^{i_l}} = \sum_{\{i_{l+1},\cdots,i_d\} \in P_k'} Y^{p^{i_l+1}+\cdots+p^{i_d}} = \#(P_k). \tag{2.43}$$

Lastly, suppose $\{i_1, \cdots, i_l\} \in P_w$ and $p^{i_1} + \cdots + p^{i_l} = e_w \neq 0 \in \mathbb{F}_r$, then $e_w \in H_s$, where $e_w = \alpha^s p^i \in \mathbb{F}_r$, some i. Further note that $e_w = p^{i_1} + \cdots + p^{i_l}$ implies $e_w p^u = p^{i_1+u} + \cdots + p^{i_l+u}$ and that, by (2.39), we have $H_s = \{e_w p^u\}_{u=0}^{d-1} = \{-e_w p^u\}_{u=0}^{d-1}$. Referring now to (2.13) and (2.37),

$$\begin{aligned}
\sum_{\{i_1,\cdots i_l\}\in P_w} Y^{p^{i_1}+\cdots+p^{i_l}} &= \sum_{u=0}^{d-1} Y^{p^{i_1+u}+\cdots+p^{i_l+u}} = \sum_{u=0}^{d-1} Y^{e_w p^u} \\
&= \sum_{u=0}^{d-1} Y^{-e_w p^u} = \sum_{u=0}^{d-1} Y^{-[p^{i_{l+1}}+\cdots+p^{i_d}]} \\
&= \sum_{u=0}^{d-1} Y^{p^u[p^{i_{l+1}}+\cdots+p^{i_d}]} \\
&= \sum_{u=0}^{d-1} Y^{p^{i_{l+1}+u}+\cdots+p^{i_d+u}} \\
&= \sum_{\{i_{l+1},\cdots,i_d\}\in P'_w} Y^{p^{i_{l+1}}+\cdots+p^{i_d}}
\end{aligned} \tag{2.44}$$

and noting that $\sum_{u=0}^{d-1} Y^{e_w p^u} = v_s$, we see that P_w yields v_s if, and only if, P'_w yields v_s.

Since $\alpha_{lk}^{(0)}$ is the number of the P_w which yield v_k and $\alpha_{d-l,k}^{(0)}$ is the number of P'_w which yield v_k, it follows that $\alpha_{lk}^{(0)} = \alpha_{d-l,k}^{(0)}$. Further, (2.42) and (2.43) show that $\beta_l^{(0)} = \beta_{d-l}^{(0)}$. Combining this result with Lemma 5 we have

$$\beta_l^{(i)} = \beta_l^{(0)} = \beta_{d-l}^{(0)} = \beta_{d-l}^{(i)} \tag{2.45}$$

and

$$\alpha_{lk}^{(i)} = \alpha_{l,k-i}^{(0)} = \alpha_{d-l,k-i}^{(0)} = \alpha_{d-l,k}^{(i)} \tag{2.46}$$

which completes the proof of the lemma. ■

Noting now that the coefficient of x^l in $g_u(x)$ is

$$(-1)^{d-l}\left(\beta_l^{(u)} + \sum_{i=0}^{m-1} \alpha_{li}^{(u)} t_i\right) \tag{2.47}$$

and that of x^{d-l} is

$$(-1)^l \left(\beta_{d-l}^{(u)} + \sum_{i=0}^{m-1} \alpha_{d-l,i}^{(u)} t_i \right) \tag{2.48}$$

then, since d even implies $d - l \equiv l \bmod 2$, hence $(-1)^{d-l} = (-1)^l$, Lemma 8 immediately yields the following corollary.

Corollary 2 *For d even, the coefficients of the $g_i(x)$, the irreducible factors of $\Phi_r(x)$, $0 \leq i \leq m-1$, are symmetric. That is, the coefficient of x^l equals the coefficient of x^{d-l}.*

As an example, note the results of the example on p. 20.

For the case where d is odd we have a similar result with a similar proof.

Lemma 9 *d odd, $d \neq 1$, then, for $s \in \mathbb{Z}/d\mathbb{Z}$, $i, k \in \mathbb{Z}/m\mathbb{Z}$, there exists $a \in \mathbb{Z}/m\mathbb{Z}$ so that*

$$\begin{aligned} \beta_l^{(i)} &= \beta_{d-l}^{(i+a)} \\ \alpha_{lk}^{(i)} &= \alpha_{d-l,k}^{(i+a)}. \end{aligned}$$

Proof: First note that, unlike the case for d even, if $p^s \equiv -1 \bmod r$, $1 < s \leq d-1$, then d divides $2s$. But d odd, so d divides s, but $0 < s < d$, a contradiction. Therefore there exists an $a \in \mathbb{Z}/m\mathbb{Z} - \{0\}$ such that $-1 \in H_a$, that is, $-1 \equiv \alpha^a p^h \bmod r$ for some $0 \leq h \leq d-1$. So we have

$$H_0 = \left\{1, p, p^2, \cdots, p^{d-1}\right\} \subseteq \mathbb{F}_r^* \tag{2.49}$$

and

$$H_a = \left\{\alpha^a p^s, \alpha^a p^{h+1}, \alpha^a p^{s+1}, \cdots, \alpha^a p^{h+d-1}\right\} \subseteq \mathbb{F}_r^* \tag{2.50}$$

and, for $0 \leq k \leq d-1$,

$$p^k = -\alpha^a p^{h+k} \in \mathbb{F}_r^*. \tag{2.51}$$

In particular,

$$\gamma \in H_0 \Leftrightarrow -\gamma \in H_a.$$

Let $I = \{i_1, \cdots, i_l\} \in \mathcal{S}$ and $I^C = \{i_{l+1}, \cdots, i_d\} \in \mathcal{S}'$. Working in $\mathbb{F}_r$, from (2.51) we have

$$p^{i_1} + \cdots + p^{i_l} = -\left(\alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l}\right) \tag{2.52}$$

and from Lemma 2 we have, since $H_a = \left\{\alpha^a, \alpha^a p, \cdots, \alpha^a p^{d-1}\right\}$ and

$$\{h+i_1, \cdots, h+i_d\} = \{0, 1, \cdots, d-1\}, \tag{2.53}$$

that

$$\alpha^a p^{h+i_1} + \cdots + \alpha^a p^{h+i_l} = -\left(\alpha^a p^{h+i_{l+1}} + \cdots + \alpha^a p^{h+i_d}\right) \tag{2.54}$$

hence

$$p^{i_1} + \cdots + p^{i_l} = \alpha^a p^{h+i_{l+1}} + \cdots + \alpha^a p^{h+i_d}. \tag{2.55}$$

If $\{i_1, \cdots, i_l\} \in \mathcal{S}_2$, then $p^{i_1} + \cdots + p^{i_l} = 0$, so $\alpha^a p^{h+i_{l+1}} + \cdots + \alpha^a p^{h+i_d} = 0$ hence $\alpha^a p^h \left(\alpha^a p^{i_{l+1}} + \cdots + \alpha^a p^{i_d}\right) = 0$ and finally, since $\alpha^a p^h \neq 0$, $\alpha^a p^{i_{l+1}} + \cdots + \alpha^a p^{i_d} = 0$. So we have $Y^{p^{i_1}+\cdots+p^{i_l}} = Y^{p^{i_{l+1}}+\cdots+p^{i_d}} = 1 \in \mathcal{R}$ and so

$$\sum_{\{i_1,\cdots,i_l\} \in S_2} Y^{p^{i_1}+\cdots+p^{i_l}} = \sum_{\{i_{l+1},\cdots,i_d\} \in S_2'} Y^{\alpha^a\left(p^{i_{l+1}}+\cdots+p^{i_d}\right)} = \#(S_2). \tag{2.56}$$

Similarly, if $\{i_1, \cdots, i_l\} \in P_k$ and $p^{i_1} + \cdots + p^{i_l} = 0 \in \mathbb{F}_r$, then

$$\sum_{\{i_1,\cdots,i_l\}\in P_k} Y^{p^{i_1}+\cdots+p^{i_l}} = \sum_{\{i_{l+1},\cdots,i_d\}\in P'_k} Y^{\alpha^a\left(p^{i_{l+1}}+\cdots+p^{i_d}\right)} = \#(P_k). \tag{2.57}$$

Lastly, suppose $\{i_1, \cdots, i_l\} \in P_w$ and $p^{i_1} + \cdots + p^{i_l} = e_w \neq 0 \in \mathbb{F}_r$, then $e_w \in H_s$ where $e_w = \alpha^s p^i \in \mathbb{F}_r$, some i, and we have

$$\begin{aligned} v_s &= \sum_{u=0}^{d-1} Y^{ep^u} = \sum_{\{i_1,\cdots,i_l\}\in P_w} Y^{p^{i_1}+\cdots+p^{i_l}} \\ &= \sum_{\{i_{l+1},\cdots,i_d\}\in P'_w} Y^{\alpha^a p^{h+i_{l+1}}+\cdots+\alpha^a p^{h+i_d}} \\ &= \sum_{\{i_{l+1},\cdots,i_d\}\in P'_w} Y^{\left(\alpha^a p^{i_{l+1}}+\cdots+\alpha^a p^{i_d}\right)} \end{aligned} \tag{2.58}$$

So P_w, thinking of $g_0(x)$, yields v_s if, and only if, P'_w, thinking of $g_a(x)$, yields v_s. Since $\alpha_{lk}^{(0)}$ is the number of the P_w from $g_{(0)}(x)$ which yield v_k and $\alpha_{d-l,k}^{(a)}$ is the number of P'_w from $g_a(x)$ which yield v_k, it follows that $\alpha_{lk}^{(0)} = \alpha_{d-l,k}^{(a)}$. Further, (2.56) and (2.57) show that $\beta_l^{(0)} = \beta_{d-l}^{(a)}$. Combining this with Lemma 5 we have

$$\beta_l^{(i)} = \beta_l^{(0)} = \beta_{d-l}^{(a)} = \beta_{d-l}^{(i+a)} \tag{2.59}$$

and

$$\alpha_{lk}^{(i)} = \alpha_{l,k-i}^{(0)} = \alpha_{d-l,k-i}^{(a)} = \alpha_{d-l,k}^{(i+a)} \tag{2.60}$$

which completes the proof of the lemma. ■

Noting now that the coefficient of x^l in $g_u(x)$ is

$$(-1)^{d-l}\left(\beta_l^{(u)} + \sum_{i=0}^{m-1} \alpha_{li}^{(u)} t_i\right) \tag{2.61}$$

and that of x^{d-l} in $g_{u+a}(x)$ is

$$(-1)^l \left(\beta_{d-l}^{(u+a)} + \sum_{i=0}^{m-1} \alpha_{d-l,i}^{(u+a)} t_i \right) \tag{2.62}$$

then, since d odd implies $d - l \not\equiv l \bmod 2$, hence $(-1)^{d-l} = -(-1)^l$, Lemma 9 immediately yields the following corollary.

Corollary 3 *For d odd, $d \neq 1$, there exists $a \in \mathbb{Z}/m\mathbb{Z}$, not zero, so that the coefficient of x^l in $g_u(x)$ equals the negative of the coefficient of x^{d-l} in $g_{u+a}(x)$.*

Note that the case $d = 1$ is the case where the degree of the irreducible factors of $\Phi_r(x)$ is 1, that is, $\Phi_r(x)$ splits completely over $\mathbb{F}_p$, and that Lemma 9 and Corollary 3 are certainly not true in this case.

Chapter 3

An Algebraic Approach

In this chapter we use many of the results of Chapter 2 to create algebraic structures to study the role of the traces of the irreducible factors of the cyclotomic polynomial.

3.1 An $\mathbb{F}_p$-algebra

In this section, using the traces and their relations as a guide, we shall construct an $\mathbb{F}_p$-algebra which is isomorphic to the Berlekamp sub-algebra of $\mathbb{F}_p[x]/\Phi_r(x)$.

Let us suppose that we have distinct primes, p and r, that $d = \text{ord}(p, r)$, $m = \frac{r-1}{d}$, that we have chosen a primitive element, α, of $\mathbb{F}_r^*$, and that we have constructed $H_0, \cdots, H_{m-1}$ as outlined in Section 2.1.

Let $\mathbb{K}$ be a splitting field for $\Phi_r(x)$ over $\mathbb{F}_p$ and let ζ be a primitive r^{th} root of unity in $\mathbb{K}$. We know that $\Phi_r(x)$ factors into the m d^{th} degree polynomials, $g_0(x), \cdots, g_{m-1}(x)$, irreducible over $\mathbb{F}_p$, as in Section 2.1. Recall that the Chinese

Remainder Theorem[1] gives an isomorphism between $\mathbb{F}_p[x]/\Phi_r(x)$ and the direct sum of splitting fields for $\Phi_r(x)$

$$\varphi : \mathbb{F}_p[x]/\Phi(x) \cong \mathbb{F}_p[x]/g_0(x) \oplus \cdots \oplus \mathbb{F}_p[x]/g_{m-1}(x) \tag{3.1}$$

by

$$f(x) + (\Phi(x)) \mapsto (f(x) + (g_0(x)), \cdots, f(x) + (g_{m-1}(x))). \tag{3.2}$$

In order to minimize confusion let us agree to represent elements of $\mathbb{F}_p[x]/\Phi(x)$ by the unique coset representative modulo $\Phi_r(x)$ which is a polynomial of degree less than $r-1$. Similarly, let us agree to represent elements of $\mathbb{F}_p[x]/g_0(x) \oplus \cdots \oplus \mathbb{F}_p[x]/g_{m-1}(x)$ by an m-tuple of polynomials whose i^{th} entry is the unique coset representative modulo $g_i(x)$ which is a polynomial of degree less than d.

Recalling the relations from the product formula, (1.8), let $\{T_i \mid i \in \mathbb{Z}/m\mathbb{Z}\}$ be indeterminates and define $R \subset \mathbb{F}_p[T_0, \cdots, T_{m-1}]$ to be the ideal generated by the set

$$\{T_i T_{i+k} - \sum_{h=0}^{m-1} [(k,h) - d\theta_k] T_{i+h} \mid i, j \in \mathbb{Z}/m\mathbb{Z}\} \cup \{1 + T_0 + \cdots + T_{m-1}\} \tag{3.3}$$

where (k,h) is the appropriate cyclotomic number and θ_k is as defined on p.6. Now we define the quotient ring

$$\mathbb{F}_p[\mathbb{T}] = \mathbb{F}_p[T_0, \cdots, T_{m-1}]/R. \tag{3.4}$$

We may think of $\mathbb{F}_p[\mathbb{T}]$ as the m-dimensional $\mathbb{F}_p$-algebra of homogeneous first degree polynomials in $T_0, \cdots, T_{m-1}$ where the ring action is given by the relations in R,

[1] See, for example, [LAN].

relations that are designed to mimic the relations given by the product rule for the periods in the theory of cyclotomy.

Let $\mathbb{K}$ be any splitting field for $\Phi_r(x)$ over $\mathbb{F}_p$ and define the polynomials

$$T_i(x) = \sum_{j=0}^{d-1} x^{\alpha^i p^j} \in \mathbb{K}[x]. \tag{3.5}$$

Now suppose that ζ is any primitive r^{th} root of unity in $\mathbb{K}$. Once again, for $i \in \mathbb{Z}/m\mathbb{Z}$, define the polynomials

$$g_i(x) = \prod_{j=0}^{d-1} \left(x - \zeta^{\alpha^i p^j}\right) \in \mathbb{F}_p[x] \subseteq \mathbb{K}[x] \tag{3.6}$$

and the traces of these polynomials

$$t_i = \sum_{j=0}^{d-1} \zeta^{\alpha^i p^j} \in \mathbb{F}_p \subseteq \mathbb{K}. \tag{3.7}$$

For $i, k \in \mathbb{Z}/m\mathbb{Z}$ we compute, for any $l \in \mathbb{Z}/d\mathbb{Z}$,

$$\begin{aligned} T_i(\zeta^{\alpha^k p^l}) &= \sum_{j=0}^{d-1} \left(\zeta^{\alpha^k p^l}\right)^{\alpha^i p^j} \\ &= \sum_{j=0}^{d-1} \left(\zeta^{\alpha^{k+i} p^{l+j}}\right) \\ &= \sum_{j=0}^{d-1} \left(\zeta^{\alpha^{k+i} p^j}\right) = t_{i+k}. \end{aligned} \tag{3.8}$$

Since the polynomial $T_i(x) - t_{i+k} \in \mathbb{F}_p[x]$ vanishes on all of the roots of $g_k(x) \in \mathbb{F}_p[x]$ there exists a polynomial $h_k(x) \in \mathbb{F}_p[x]$ so that

$$T_i(x) = g_k(x)h_k(x) + t_{i+k}. \tag{3.9}$$

Now let $\overline{T_i(x)}$ be the projection of $T_i(x) \in \mathbb{F}_p[x]$ into $\mathbb{F}_p[x]/\Phi_r(x)$ and let φ be the isomorphism in (3.1). Then, for $i \in \mathbb{Z}/m\mathbb{Z}$ we have

$$\varphi(\overline{T_i(x)}) = (t_i, t_{i+1}, \cdots, t_{i-1}) \tag{3.10}$$

where it is understood that the j^{th} entry of the m-tuple is a coset representative mod $g_j(x)$.

An interesting by-product of this observation is the following.

Corollary 4 *Given distinct primes p and r with $d = ord(p,r) \neq 1$, then, in any p-cycle* mod r, *there is at least one element that is greater than d. That is, every coset of the subgroup of $\mathbb{F}_r^*$ generated by the least residue of p* mod r *contains at least one of $\{d+1, d+2, \cdots, r-1\}$.*

Proof: Choose $i \in \mathbb{Z}/m\mathbb{Z}$, we must show that H_i contains an element greater than d. Recall that we labeled the cosets of $< p >$ in $\mathbb{F}_r^*$ by $H_0, H_1, \cdots, H_{m-1}$, where $H_0 =< p >$ and $H_i = \alpha^i H_0$. If $r-1 \in H_i$, then, as $r-1 > d$, we are done. Otherwise, from (3.9) we know that $\sum_{k\in H_i} x^k \equiv t_i \bmod g_0(x)$ and, since $\sum_{k\in H_i} x^k$ is not a constant polynomial and $t_i \in \mathbb{F}_p$, it follows that

$$\deg\left(\sum_{k\in H_i} x^k\right) = \max\{k | k \in H_i\} \geq \deg\ g_0(x) = d \tag{3.11}$$

hence some element of H_i is greater than or equal to d.

If $\deg\left(\sum_{k\in H_i} x^k\right) = d$, then, for any $l \in \mathbb{Z}/m\mathbb{Z}$, as both $\sum_{k\in H_i} x^k$ and $g_l(x)$ are monic, it follows from (3.9) that

$$T_i(x) = \sum_{k\in H_i} x^k = g_l(x) + t_{i+l}. \tag{3.12}$$

Therefore $g_0(x) - g_l(x) = t_{i+l} - t_i$ for all $l \in \mathbb{Z}/m\mathbb{Z}$. By Corollaries 1 and 3 it follows that the constant terms of $g_0(x)$ and $g_l(x)$ are both the same, hence we must have that x divides $g_0(x) - g_l(x)$, so x divides $t_{i+l} - t_i$ for all $l \in \mathbb{Z}/m\mathbb{Z}$, which implies that all of the traces are the same. We shall see in Lemma 13 that this cannot be the case. Therefore $\deg\left(\sum_{k\in H_i} x^k\right) \neq d$ and so there exists $k \in H_i$ such that $k > d$. ■

We have the same relations among the $\overline{T_i(x)}$ as we do among the $T_i \in \mathbb{F}_p[\mathbb{T}]$. Given $\overline{T_i(x)}$ and $\overline{T_j(x)}$ note that

$$\begin{aligned}
& \varphi\left(\overline{T_i(x)T_{i+k}(x)}\right) \\
= \; & (t_i t_{i+k}, t_{i+1}t_{i+1+k}, \cdots, t_{i-1}t_{i-1+k}) \\
= \; & \left(\sum_{h=0}^{m-1}[(k,h) - d\theta_k]t_{i+h}, \sum_{h=0}^{m-1}[(k,h) - d\theta_k]t_{i+1+h}, \cdots, \right. \\
& \qquad \left. \sum_{h=0}^{m-1}[(k,h) - d\theta_k]t_{i-1+h}\right) \qquad (3.13) \\
= \; & \sum_{h=0}^{m-1}\left([(k,h) - d\theta_k]\,(t_{i+h}, t_{i+1+h}, \cdots, t_{i-1+h})\right) \\
= \; & \sum_{h=0}^{m-1}\left([(k,h) - d\theta_k]\varphi\left(\overline{T_{i+h}(x)}\right)\right)
\end{aligned}$$

hence, since φ is an isomorphism,

$$\overline{T_i(x)T_{i+k}(x)} = \sum_{h=0}^{m-1}\left([(k,h) - d\theta_k]\overline{T_{i+h}(x)}\right). \qquad (3.14)$$

Now define $\psi : \mathbb{F}_p[\mathbb{T}] \to \mathbb{F}_p[x]/\Phi_r(x)$ by

$$\psi : \sum_{i=0}^{m-1}\alpha_i T_i \mapsto \sum_{i=0}^{m-1}\alpha_i\overline{T_i(x)}. \qquad (3.15)$$

Lemma 10 *ψ is an injective $\mathbb{F}_p$-algebra homomorphism.*

Proof: Define the homomorphism $\gamma : \mathbb{F}_p[T_0, \cdots, T_{m-1}] \rightarrow \mathbb{F}_p[x]/\Phi(x)$ by $T_i \mapsto \overline{T_i(x)}$ and note that (3.3) and (3.14) above show that $\varphi(R) = 0$, so γ factors through $\mathbb{F}_p[\mathbb{T}]$ via ψ, hence ψ is an $\mathbb{F}_p$-algebra homomorphism.

To see that ψ is injective let us stray momentarily from our agreement regarding the representation of elements in $\mathbb{F}_p[x]/\Phi_r(x)$ and note that, modulo $\Phi_r(x)$, any polynomial has a unique representation as an $r-1^{st}$ degree polynomial without a constant term. Specifically, since $x^r \equiv 1 \bmod \Phi_r(x)$, we have, for $\beta_1 \equiv \beta_2 \bmod r$, that $x^{\beta_1} \equiv x^{\beta_2} \bmod \Phi_r(x)$ and that $1 \equiv -x - x^2 - \cdots - x^{r-1} \bmod \Phi_r(x)$. Now note that the $T_i(x) = \sum_{j=0}^{d-1} x^{\alpha^i p^j}$ where, for $0 \leq j \leq d-1$, $\alpha^i p^j \neq 0 \in \mathbb{F}_r$ [since the order of $p \bmod r$ is d]. Therefore, using the representation above, we write

$$\overline{T_i(x)} = \sum_{j=0}^{d-1} x^{\overline{\alpha^i p^j}} + (\Phi_r(x)) \tag{3.16}$$

where $\overline{\alpha^i p^j}$ is the least residue of $\alpha^i p^j \bmod r$. If we now remark that, for $0 \leq i < k \leq m-1$, $\alpha^i p^{l_1} \not\equiv \alpha^k p^{l_2} \bmod r$ for any l_1 and l_2, then there can be no non-trivial relations among the $\overline{T_i(x)}$. That is, $\overline{T_0(x)}, \cdots, \overline{T_{m-1}(x)}$ have distinct representations as polynomials of degree less than r, no constant term, and that

no two of these representations have terms of equal degree, so the only linear combinations of these elements which equals zero is the trivial one. Therefore

$$\psi\left(\sum_{i=0}^{m-1}\alpha_i T_i\right)=\sum_{i=0}^{m-1}\alpha_i\overline{T_i(x)}=0\Leftrightarrow\alpha_i=0\ \forall i\in\mathbb{Z}/m\mathbb{Z} \tag{3.17}$$

and so ψ is injective. ■

It is interesting to remark at this point that a direct sum of m copies of $\mathbb{F}_p$, call it $\mathcal{B}$, also known as the *Berlekamp sub-algebra*[1] sits inside of $\mathbb{F}_p[x]/g_0(x)\oplus\cdots\oplus\mathbb{F}_p[x]/g_{m-1}(x)$ in a natural way and that $\mathrm{Im}(\varphi\psi)$ is contained in this sum. As ψ is injective and $\#\left(\mathbb{F}_p[\mathbb{T}]\right)=\#\left(\mathbb{F}_p\oplus\cdots\oplus\mathbb{F}_p\right)=p^m$, finite, it follows that $\varphi\psi$ is an isomorphism from $\mathbb{F}_p[\mathbb{T}]$ to $\mathcal{B}$.

$$\begin{array}{ccc}
\mathbb{F}_p[T_0,\cdots,T_{m-1}] & & \\
\downarrow & \searrow & \\
\mathbb{F}_p[\mathbb{T}] & \xrightarrow{\psi} & \mathbb{F}_p[x]/\Phi_r(x) \\
 & & \| \varphi \\
 & \overset{\varphi\psi}{\searrow} & \oplus_{i=0}^{m-1}\frac{\mathbb{F}_p[x]}{g_i(x)} \\
 & & \cup \\
 & & \mathcal{B}
\end{array} \tag{3.18}$$

[1] See, for example, Section 2.4 of [MEN]

3.2 Some automorphisms

In this section we construct automorphisms of $\mathbb{F}_p[\mathbb{T}]$ and $\mathbb{F}_p[x]/\Phi_r(x)$ and examine some resulting module structure.

Note that the $\mathbb{F}_p$-map $\mathbb{F}_p[T_0,\cdots,T_m] \to \mathbb{F}_p[T_0,\cdots,T_m]$, by $T_i \mapsto T_{i+1}$, is clearly an $\mathbb{F}_p$-algebra automorphism. Now observe that if $f(x)$ is an element of the set which generates R, the relations ideal defined in (3.3), then the image of $f(x)$ under this map is either

$$\begin{aligned} & T_iT_{i+k} - \sum_{h=0}^{m-1}[(k,h) - d\theta_k]T_{i+h} \qquad (3.19) \\ \mapsto\ & T_{i+1}T_{(i+1)+k} - \sum_{h=0}^{m-1}[(k,h) - d\theta_k]T_{(i+1)+h} \in R \end{aligned}$$

or

$$1 + T_0 + T_1 + \cdots + T_{m-1} \mapsto 1 + T_0 + T_1 + \cdots + T_{m-1} \in R. \qquad (3.20)$$

As the image of R under this map is R, it follows that it induces an $\mathbb{F}_p$-algebra automorphism, the 'shift' automorphism, τ, on $\mathbb{F}_p[\mathbb{T}] = \mathbb{F}_p[T_0,\cdots,T_m]/R$ by $T_i \mapsto T_{i+1}$.

To mimic this action in $\mathbb{F}_p[x]/(\Phi_r(x))$ consider the $\mathbb{F}_p$-module map of $\mathbb{F}_p[x]$ given by $\lambda : x \mapsto x^\alpha$ and note that under this map the image of $\Phi_r(x)$ is

$$\lambda(\Phi_r(x)) = \sum_{i=0}^{r-1} x^{\alpha^i}. \qquad (3.21)$$

Now, as r is prime and $0 < \alpha < r-1$, it follows that $\{\alpha^0, \alpha, \cdots, \alpha^{r-1}\}$ is a complete set of residues mod r. Therefore if ζ is any primitive r^{th} root of unity over $\mathbb{F}_p$, then

$\{\zeta, \zeta^2, \cdots, \zeta^{r-1}\}$ are precisely the primitive r^{th} roots of unity over $\mathbb{F}_p$, hence we have that

$$\lambda(\Phi_r(x))(\zeta) = \sum_{i=0}^{r-1} \zeta^{\alpha^i} = \sum_{i=0}^{r-1} \zeta^i = 0. \tag{3.22}$$

Since the roots of $\Phi_r(x)$ are exactly the primitive r^{th} roots of unity, we have that $\Phi_r(x)$ divides $\lambda(\Phi_r(x))$, that is, $\lambda(\Phi_r(x)) \in (\Phi_r(x))$. So we see that λ induces an $\mathbb{F}_p$-algebra endomorphism, σ, of $\mathbb{F}_p[x]/(\Phi_r(x))$ by $\overline{x} \mapsto \overline{x^\alpha}$. Further observing that

$$\sigma\left(\left\{1, \overline{x}, \overline{x^2}, \cdots, \overline{x^{r-1}}\right\}\right) = \left\{1, \overline{x}, \overline{x^2}, \cdots, \overline{x^{r-1}}\right\} \tag{3.23}$$

we see that σ is onto hence, as $\mathbb{F}_p[x]/(\Phi_r(x))$ is finite, an $\mathbb{F}_p$-algebra automorphism of $\mathbb{F}_p[x]/(\Phi_r(x))$.

We now observe that

$$\begin{aligned} \varphi\tau(T_i) &= \varphi(T_{i+1}) = \overline{T_{i+1}(x)} \\ &= \sum_{h=0}^{m-1} x^{\alpha^{i+1}p^h} = \sigma\left(\sum_{h=0}^{m-1} x^{\alpha^i p^h}\right) \\ &= \sigma(\overline{T_i(x)}) = \sigma\varphi(T_i). \end{aligned}$$

As $\{T_0, T_1, \cdots, T_{m-1}\}$ forms a basis for $\mathbb{F}_p[\mathbb{T}]$ over $\mathbb{F}_p$ we have that

$$\varphi\tau^k = \sigma^k\varphi \tag{3.24}$$

for any k.

It should also be noted that, as $\tau^m = \mathrm{Id}_{\mathbf{F}_p[\mathbb{T}]}$, we have that τ makes $\mathbb{F}_p[\mathbb{T}]$ into an $\mathbb{F}_p[x]/(x^m - 1)$ module, where the action is given by τ.

Lemma 11 $\mathbb{F}_p[\mathbb{T}]$ *is a cyclic* $\mathbb{F}_p[x]/(x^m-1)$ *module, where the action of* $\mathbb{F}_p[x]/(x^m-1)$ *on* $\mathbb{F}_p[\mathbb{T}]$ *is given by* τ.

Proof: Simply noting that,

$$\left(\sum_{i=0}^{m-1} \alpha_i x^i\right) T_0 = \sum_{i=0}^{m-1} \alpha_i T_i \tag{3.25}$$

and that, since $T_0, T_1, \cdots, T_{m-1}$ forms a basis for $\mathbb{F}_p[\mathbb{T}]$ over $\mathbb{F}_p$, it follows that, as an $\mathbb{F}_p[x]/(x^m-1)$ module,

$$\mathbb{F}_p[\mathbb{T}] = [\mathbb{F}_p[x]/(x^m-1)]\, T_0 \tag{3.26}$$

This completes the proof. ■

A related result comes from examining the linear transformation $\lambda^m : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$ by $x \mapsto x^{a^m}$. For $a \in \mathbb{Z}$ define $\bar{a}$ to be the least positive residue of $a \bmod r$, then, since $x^r \equiv 1 \bmod \Phi_r(x)$, we know that $x^a \equiv x^{\bar{a}} \bmod \Phi_r(x)$. Now, given

$$f(x) = \sum_{i=0}^{t} \alpha_i x^i \in \mathbb{F}_p[x] \tag{3.27}$$

we define

$$f^+(x) = \sum_{i=0}^{t} \alpha_i x^{\bar{i}} \in \mathbb{F}_p[x]. \tag{3.28}$$

The remarks above show that $f \equiv f^+ \bmod \Phi_r(x)$. Further, define

$$f^*(x) = (\lambda^m f)^+ \in \mathbb{F}_p[x] \tag{3.29}$$

and note that, as $(\lambda^m f)^+ \equiv \lambda^m f \bmod \Phi_r(x)$, we have that $f^* \equiv \lambda^m f \bmod \Phi_r(x)$.

Lemma 12 *Let* $f(x) = \sum_{i=0}^{t} \alpha_i x^i \in \mathbb{F}_p[x]$. *If* $f(x)$ *divides* $\Phi_r(x)$ *then* $f(x)$ *divides* $f^*(x)$.

Proof: First note that as α^m and p both have $\text{ord}(d, r)$ it follows that they both generate the unique multiplicative subgroup of order d in $\mathbb{F}_r^*$. So there must be a q such that $p^q \equiv \alpha^m \bmod r$, hence, for any i, we have that $ip^q \equiv i\alpha^m \bmod r$ and so

$$\lambda^m f = \sum_{i=0}^{t} \alpha_i x^{i\alpha^m} \equiv \sum_{i=0}^{t} \alpha_i x^{p^q} \bmod \Phi_r(x) \tag{3.30}$$

and, since $f^* = (\lambda^m f)^+ \equiv \lambda^m f \bmod \Phi_r(x)$, we also have that

$$f^*(x) \equiv \sum_{i=0}^{t} \alpha_i x^{p^q} \bmod \Phi_r(x). \tag{3.31}$$

Further noting that, as we are in characteristic p, we have

$$f^{p^q}(x) = \sum_{i=0}^{t} \alpha_i x^{p^q} \in \mathbb{F}_p[x]$$

so it follows that $f^{p^q}(x) \equiv f^* \bmod \Phi_r(x)$. Therefore there exists $\beta \in \mathbb{F}_p[x]$ such that $f^{p^q}(x) - f^* = \beta\Phi_r(x)$. Now, if $f(x)$ divides $\Phi_r(x)$ it follows that $f(x)$ divides $f^*(x)$. ■

Please note that the converse of the above lemma is not generally true. For example, if $\alpha^m \not\equiv -1 \bmod r$ then x divides x^* and yet x does not divide $\Phi_r(x)$.

3.3 Idempotents

In this section we shall examine several ideas for factoring $\Phi_r(x)$ given one or more of the traces of the irreducible factors of $\Phi_r(x)$. The reader may note that this

material is similar to methods involving Berlekamp's algorithm discussed in Chapter 4 of [LID1], the main difference being the attention given to the role that the traces of the irreducible factors of $\Phi_r(x)$ can play.

Note that every idempotent in $\mathbb{F}_p[x]/g_0(x) \oplus \cdots \oplus \mathbb{F}_p[x]/g_{m-1}(x)$ must be of the form $(a_0, \cdots, a_{m-1})$, where $a_i = 0$ or 1, $i \in \mathbb{Z}/m\mathbb{Z}$, and that the set of all idempotents is in $\mathcal{B}$ and therefore in one-to-one correspondence, via the isomorphism $\varphi\psi$, with the idempotents in $\mathbb{F}_p[\mathbb{T}]$. We also note that every zero divisor in $\mathbb{F}_p[x]/g_0(x) \oplus \cdots \oplus \mathbb{F}_p[x]/g_{m-1}(x)$ must be of the form $(a_0, \cdots, a_{m-1})$ where there is some i so that $a_i \not\equiv 0 \bmod g_i(x)$ and some j so that $a_j \equiv 0 \bmod g_j(x)$. If $a(x) + (\Phi_r(x)) = \varphi^{-1}((a_0, \cdots, a_{m-1}))$ then it follows that $\gcd(a(x), \Phi_r(x)) \neq 1$ or $\Phi_r(x)$, hence yields a non-trivial factorization of $\Phi_r(x)$.

We may also define the *principal idempotents*

$$e_i = (1 - \delta_{0i}, 1 - \delta_{1i}, \cdots, 1 - \delta_{m-1,i}) \in \mathcal{B} \tag{3.32}$$

for each $i \in \mathbb{Z}/m\mathbb{Z}$ where δ_{ij} is Kronecker's delta. If we let $e_i(x) \in \mathbb{F}_p[x]$ be the unique coset representative of $\varphi^{-1}(e_i)$ with degree less than $r - 1$, then

$$\begin{aligned} e_i(x) &\equiv 1 \bmod g_j(x),\ i \neq j \\ e_i(x) &\equiv 0 \bmod g_i(x) \end{aligned} \tag{3.33}$$

hence $\gcd(\Phi_r(x), e_i(x)) = g_i(x)$. Alternatively, if we define $e_i'(x) \in \mathbb{F}_p[x]$ to be the unique coset representative of degree less than $r - 1$ of $\varphi^{-1}(1 - e_i)$ then $g_i(x) =$

$\Phi_r(x)/\gcd(\Phi_r(x), e_i'(x))$.

Keeping in mind the one-to-one correspondence of idempotents in $\mathbb{F}_p[\mathbb{T}]$ and those in $\mathcal{B}$, we see that any idempotent in $\mathbb{F}_p[\mathbb{T}]$ will give a non-trivial factorization of $\Phi_r(x)$ and given any of the $e_i(x)$ we will get an irreducible factor of $\Phi_r(x)$. Given all of the principal idempotents gives a complete factorization of $\Phi_r(x)$.

Suppose that we happen to know one of the traces, t_i. Then $\varphi\left(\overline{T_0(x)} - t_i\right) = (t_0 - t_i, \cdots, t_{m-1} - t_i) \in \mathcal{B}$ has a zero in the i^{th} position. This element will be zero if, and only if, all of the t_i are equal.

Lemma 13 *Given distinct primes, r and p, the traces of the irreducible factors of $\Phi_r(x)$ cannot all be the same.*

Proof: As remarked above, if the traces were all the same then $\overline{T_0(x)} - t_i = 0 \in \mathbb{F}_p[x]/\Phi_r(x)$. Recalling the representation of elements in $\mathbb{F}_p[x]/\Phi_r(x)$ discussed in the proof of Lemma 10 we may represent $\overline{T_0(x)} - t_i$ by

$$\overline{T_0(x)} - t_i = \sum_{j=0}^{d-1} x^{\overline{p^j}} + t_i \sum_{j=1}^{r-1} x^j = \sum_{j=1}^{r-1} s_j x^j \tag{3.34}$$

where $\overline{p^j}$ is the least residue of p^j mod r and

$$s_j = \begin{cases} 1 + t_i \text{ if } j \in H_0 \\ t_i, \text{ otherwise} \end{cases} . \tag{3.35}$$

This element will be 0 if, and only if, $s_j = 0$ for all $0 \leq j \leq r-1$. As some j are in H_0 and some are not, this would simultaneously force $t_i = 1$ and $t_i = 0$. ■

So $\overline{T_0(x)} - t_i$ will be a non-trivial zero divisor. It should further be noted that

$$\left(\varphi\left(\overline{T_0(x)} - t_i\right)\right)^{p-1} = \left((t_0 - t_i)^{p-1}, \cdots, (t_{m-1} - t_i)^{p-1}\right) \tag{3.36}$$

where, since we are working in characteristic p, $(t_j - t_i)^{p-1} = 0$ or 1 as $t_j = t_i$ or not, respectively. As $\left(\overline{T_0(x)} - t_i\right)^{p-1}$ can be computed in $\log p$ multiplications it follows that we will have found a non-trivial idempotent of $\mathcal{B}$ in polynomial time. Whether working with the idempotent or the zero divisor we will have a non-trivial factorization of $\Phi_r(x)$.

It is a well known fact[1] that if $f(x)$ is any polynomial over any finite field $\mathbb{F}_q$, and if $b(x)$ is an element of the Berlekamp sub-algebra of $\mathbb{F}_q[x]/f(x)$, then we have

$$f(x) = \prod_{a \in \mathbb{F}_q} \gcd\left(f(x), b(x) - a\right). \tag{3.37}$$

Noting that $\overline{T_0(x)}$ is an element of the Berlekamp sub-algebra of $\mathbb{F}_q[x]/\Phi_r(x)$ we have

$$\Phi_r(x) = \prod_{a \in \mathbb{F}_p} \gcd\left(\Phi_r(x), \overline{T_0(x)} - a\right). \tag{3.38}$$

If we now observe that $\gcd\left(\Phi_r(x), \overline{T_0(x)} - a\right) = 1$ for a$\notin \{t_0, \cdots, t_{m-1}\}$ and that $\gcd\left(\Phi_r(x), \overline{T_0(x)} - t_i\right)$ is a proper, non-trivial factor of $\Phi_r(x)$ for $i = 0, \cdots, m-1$, (3.38) becomes

$$\Phi_r(x) = \prod_{i=0}^{m-1} \gcd\left(\Phi_r(x), \overline{T_0(x)} - t_i\right). \tag{3.39}$$

Noting that these gcd calculations can be done in time $r^{O(1)}$ we see that if we know

[1] See, for example, Section 2.4 of [MEN]

all of the traces of the irreducible factors of $\Phi_r(x)$ then we may compute the complete factorization of $\Phi_r(x)$ deterministically in time $r^{O(1)}$.

Also note that for any i, $\sigma^j\left(\overline{T_0(x)} - t_i\right) = \overline{T_j(x)} - t_i$ will also be a zero divisor, so we may get other non-trivial factorizations of $\Phi_r(x)$. In particular, if t_i is distinct from all of the other traces then $\left\{\left(\overline{T_j(x)} - t_i\right)^{p-1}\right\}_{j=0}^{m-1}$ are precisely the m principal idempotents and we will have a complete factorization of $\Phi_r(x)$ via

$$\Phi_r(x) = \prod_{j=0}^{m-1} \gcd\left(\Phi_r(x), \overline{T_j(x)} - t_i\right). \tag{3.40}$$

Example: Let $p = 53$ and $r = 29$, then $m = 4$, $d = 7$ and we may choose $\alpha = 2$. As outlined in Chapter 1 we find

$$\begin{aligned} H_0 &= \{1, 24, 25, 20, 16, 7, 23\} \\ H_1 &= \{2, 19, 21, 11, 3, 14, 7\} \\ H_2 &= \{4, 9, 13, 22, 6, 28, 5\} \\ H_3 &= \{8, 18, 26, 15, 12, 27, 10\} \end{aligned} \tag{3.41}$$

hence

$$\begin{aligned} \overline{T_0(x)} &= x + x^{24} + x^{25} + x^{20} + x^{16} + x^7 + x^{23} + (\Phi_{29}) \\ \overline{T_1(x)} &= x^2 + x^{19} + x^{21} + x^{11} + x^3 + x^{14} + x^7 + (\Phi_{29}) \\ \overline{T_2(x)} &= x^4 + x^9 + x^{13} + x^{22} + x^6 + x^{28} + x^5 + (\Phi_{29}) \\ \overline{T_3(x)} &= x^8 + x^{18} + x^{26} + x^{15} + x^{12} + x^{27} + x^{10} + (\Phi_{29}). \end{aligned} \tag{3.42}$$

Given that one of the traces, which we arbitrarily assign as t_0, of the irreducible

factors of $\Phi_{29}(x)$ over $\mathbb{F}_{53}$ is 33, then we know that both

$$\begin{aligned} T_0 - 33 &= 21T_0 + 20T_1 + 20T_2 + 20T_3 \\ \overline{T_0(x)} - 33 &= x + x^{24} + x^{25} + x^{20} + x^{16} + x^7 + x^{23} - 33 + (\Phi_{29}) \end{aligned} \tag{3.43}$$

are zero divisors. We then compute

$$\begin{aligned} &\gcd(\Phi_{29}(x), x + x^{24} + x^{25} + x^{20} + x^{16} + x^7 + x^{23} - 33) \\ &= x^7 + 20x^6 + 16x^5 + 4x^4 + 38x^3 + 34x^2 + 36x + 52 \end{aligned} \tag{3.44}$$

As this polynomial is of degree seven and necessarily divisible by $g_0(x)$ it follows that it is $g_0(x)$. Computing $\gcd(\Phi_{29}(x), \overline{T_i(x)} - 33)$ for $i = 1, 2, 3$ in turn we find

$$\begin{aligned} g_1(x) &= x^7 + 14x^6 + 2x^5 + 21x^4 + 35x^3 + 40x^2 + 50x + 52 \\ g_2(x) &= x^7 + 17x^6 + 19x^5 + 15x^4 + 49x^3 + 37x^2 + 33x + 52 \\ g_3(x) &= x^7 + 3x^6 + 13x^5 + 18x^4 + 32x^3 + 51x^2 + 39x + 52. \end{aligned} \tag{3.45}$$

and we have a complete factorization of $\Phi_{29}(x)$ over $\mathbb{F}_{53}$. Note that we have also learned that $t_1 = 39$, $t_2 = 36$ and that $t_3 = 50$.

If we further compute $(T_0 - 33)^{52}$ in $\mathbb{F}_{53}[\mathbb{T}]$ and apply σ to this element three times, we find that the principal idempotents in $\mathbb{F}_{53}[\mathbb{T}]$ are

$$\begin{aligned} &51T_0 + 3T_1 + 31T_2 + 18T_3 \\ &3T_0 + 31T_1 + 18T_2 + 51T_3 \\ &31T_0 + 18T_1 + 51T_2 + 3T_3 \\ &18T_0 + 51T_1 + 3T_2 + 31T_3. \end{aligned} \tag{3.46}$$

Applying ψ to each of these in turn we may also find the principal idempotents in $\mathbb{F}_{53}[x]/\Phi_{29}(x)$. ■

But what if the traces are not all distinct? Note that this will certainly be the case when $p < d$ and even occurs, though infrequently, for $p > r$. Experimentation has revealed that even when traces repeat we may still get a set of factors which separate $\Phi_r(x)$. However, this need not always happen.

Example: If we let $p = 137$ and $r = 101$ we find $d = 5$ and $m = 20$. So $\Phi_r(x)$ will factor into 20 distinct irreducible polynomials each of degree 5. It turns out the that the number $t = 71$ occurs as a trace for two of these polynomials. Computing $f_i(x) = \gcd\left(\Phi_{101}(x), \overline{T_j(x)} - 71\right)$ for $j = 0, \cdots, 19$ we find only 10 distinct 10^{th} degree polynomials (only the coefficients of $1, x, \cdots, x^{10}$, respectively, are shown below),

$$
\begin{aligned}
f_0(x) &= 1 \;\; 132 \;\; 94 \;\; 121 \;\; 72 \;\; 38 \;\; 72 \;\; 121 \;\; 94 \;\; 132 \;\; 1 \\
f_1(x) &= 1 \;\; 4 \;\; 74 \;\; 111 \;\; 82 \;\; 85 \;\; 82 \;\; 111 \;\; 74 \;\; 4 \;\; 1 \\
f_2(x) &= 1 \;\; 57 \;\; 51 \;\; 96 \;\; 30 \;\; 115 \;\; 30 \;\; 96 \;\; 51 \;\; 57 \;\; 1 \\
f_3(x) &= 1 \;\; 30 \;\; 136 \;\; 43 \;\; 82 \;\; 116 \;\; 82 \;\; 43 \;\; 136 \;\; 30 \;\; 1 \\
f_4(x) &= 1 \;\; 93 \;\; 24 \;\; 32 \;\; 16 \;\; 98 \;\; 16 \;\; 42 \;\; 32 \;\; 93 \;\; 1 \\
f_5(x) &= 1 \;\; 6 \;\; 133 \;\; 15 \;\; 94 \;\; 80 \;\; 94 \;\; 15 \;\; 133 \;\; 6 \;\; 1 \\
f_6(x) &= 1 \;\; 59 \;\; 31 \;\; 98 \;\; 25 \;\; 112 \;\; 25 \;\; 98 \;\; 31 \;\; 59 \;\; 1 \\
f_7(x) &= 1 \;\; 29 \;\; 39 \;\; 26 \;\; 9 \;\; 103 \;\; 9 \;\; 26 \;\; 39 \;\; 29 \;\; 1 \\
f_8(x) &= 1 \;\; 113 \;\; 97 \;\; 51 \;\; 119 \;\; 74 \;\; 119 \;\; 51 \;\; 97 \;\; 113 \;\; 1 \\
f_9(x) &= 1 \;\; 26 \;\; 52 \;\; 104 \;\; 99 \;\; 6 \;\; 99 \;\; 104 \;\; 52 \;\; 26 \;\; 1
\end{aligned}
$$

and that $f_{10} = f_0$, $f_{11} = f_1$, etcetera. We further find that $\gcd(f_i(x), f_j(x)) = 1$ for $i \not\equiv j \bmod 10$ and that in fact, subject to the appropriate ordering, we have

$$
\begin{aligned}
f_0(x) &= g_0(x)g_{10}(x) \\
f_1(x) &= g_1(x)g_{11}(x) \\
&\vdots \\
f_9(x) &= g_9(x)g_{19}(x)
\end{aligned}
$$

and so in this case we find that (3.40), although yielding non-trivial factorizations of $\Phi_{101}(x)$, does not give a complete factorization. ■

Of course, all of the above assumes that we know at least one of the traces. How can we find idempotents or zero divisors in general? If any of the t_i are 0, which is the case if, and only if, one, hence all, of the T_i are zero divisors, then we will be able to get at least partial factorizations simply by computing $\gcd\left(\Phi_r(x), \overline{T_i(x)}\right)$. If the T_i are not zero divisors then, as $\mathbb{F}_p[\mathbb{T}]$ is finite, they are units and, by recalling the isomorphism $\varphi\psi(T_i) = (t_i, t_{i+1}, \cdots, t_{i-1}) \in \mathcal{B}$, we see that the order of the $T_i's$ are all the same and that

$$\text{order } T_i = \text{lcm}(\text{ord}(t_0, p), \text{ord}(t_1, p), \cdots, \text{ord}(t_{m-1}, p)). \tag{3.47}$$

Although not always the case, experimentation shows that often, especially with large m, the $t_i's$ will not all have the same order. If we knew that some trace t had order k and that order $T_i > k$, then it would follow that $T_i^k - 1$ would be a zero divisor.

3.4 Extending $\mathbb{F}_p[\mathbb{T}]$

We have shown that $\mathbb{F}_p[\mathbb{T}]$ is isomorphic to $\mathcal{B}$ in $\mathbb{F}_p[x]/\Phi_r(x)$. We now extend $\mathbb{F}_p[\mathbb{T}]$ to an $\mathbb{F}_p$-algebra which is isomorphic to $\mathbb{F}_p[x]/\Phi_r(x)$.

Recall from Chapter 2 that we may deterministically, and in time $r^{O(1)}$, express the coefficients of the $g_i(x)$ as linear combinations of $t_0, \cdots, t_{m-1}$. Using the homogenous representation from (2.26) we know that the coefficient of x^s in $g_u(x)$ is

$$(-1)^{d-s}\left[\sum_{i=0}^{m-1} \delta_{si}^{(u)} t_i\right]. \tag{3.48}$$

Define, in $\mathbb{F}_p[\mathbb{T}]$,

$$\Gamma_{us} = (-1)^{d-s}\left[\sum_{i=0}^{m-1}\delta_{si}^{(u)}T_i\right]. \tag{3.49}$$

Let Y be an indeterminate and consider the polynomial ring $\mathbb{F}_p[\mathbb{T}][Y]$, the ring of polynomials in Y with coefficients in $\mathbb{F}_p[\mathbb{T}]$. In this ring define

$$G_u(Y) = \sum_{s=0}^{d-1}\Gamma_{us}Y^s. \tag{3.50}$$

Note that we have an $\mathbb{F}_p$-algebra homomorphism

$$\Delta : \mathbb{F}_p[\mathbb{T}][Y] \to \mathbb{F}_p[x]/\Phi_r(x) \tag{3.51}$$

by $Y \mapsto x$ and, for $\beta \in \mathbb{F}_p[\mathbb{T}]$, $\beta \mapsto \psi(\beta)$. We wish to examine the image of $G_u(Y)$ under this map, followed by the isomorphism φ into $\mathbb{F}_p[x]/g_0(x)\oplus\cdots\oplus\mathbb{F}_p[x]/g_{m-1}(x)$. To do this, let us consider the $\mathbb{F}_p$-algebra homomorphism from $\mathbb{F}_p[\mathbb{T}][Y] \to \mathbb{F}_p[x]$ given by $Y \mapsto x$ and $T_j \mapsto T_j(x)$ and regard the image mod $g_k(x)$.

First note that

$$\Gamma_{us} \mapsto (-1)^{d-s}\left(\sum_{i=0}^{m-1}\delta_{si}^{(u)}T_i(x)\right). \tag{3.52}$$

Recalling now that $T_i(x) \equiv t_{i+k} \bmod g_k(x)$ we have that the image of Γ_{us} mod $g_k(x)$ is

$$(-1)^{d-s}\left(\sum_{i=0}^{m-1}\delta_{si}^{(u)}t_{i+k}\right) \tag{3.53}$$

Now, recalling from (2.27) that $\delta_{s,t-k}^{(u)} = \delta_{st}^{(u+k)}$, we have that the image of Γ_{us} mod $g_k(x)$ is

$$\begin{aligned}(-1)^{d-s}\left(\sum_{i=0}^{m-1}\delta_{si}^{(u)}t_{i+k}\right) &= (-1)^{d-s}\sum_{i=0}^{m-1}\delta_{si-k}^{(u)}t_i \\ &= (-1)^{d-s}\left(\sum_{i=0}^{m-1}\delta_{si}^{(u+k)}t_i\right) \\ &= \delta_{u+k,s}\end{aligned} \tag{3.54}$$

the coefficient of x^s in $g_{u+k}(x)$. So we observe that the image of $G_u(Y)$ mod $g_k(x)$ is

$$\sum_{s=0}^{d-1}(-1)^{d-s}\Gamma_{us}x^s = \sum_{s=0}^{d-1}\delta_{u+k,s}x^s = g_{u+k}(x). \tag{3.55}$$

So the image of $G_u(Y)$ into $\mathbb{F}_p[x]/g_0(x) \oplus \cdots \oplus \mathbb{F}_p[x]/g_{m-1}(x)$ is

$$G_u(Y) \mapsto (g_u(x), g_{u+1}(x), \cdots, g_{u-1}(x)). \tag{3.56}$$

In particular, note that $G_0(Y) \mapsto (g_0(x), g_1(x), \cdots, g_{m-1}(x)) = 0$, hence we have an induced $\mathbb{F}_p$-algebra homomorphism

$$\Psi : \mathbb{F}_p[\mathbb{T}][Y]/(G_0(Y)) \to \mathbb{F}_p[x]/(\Phi_r(x)). \tag{3.57}$$

Noting that $\Psi(-T_0 - T_1 - \cdots - T_{m-1}) = 1$ and that $\Psi(Y) = x$, it follows that Ψ is onto. If we further observe that both rings have cardinality p^r we have proven the following.

Lemma 14 *The map*

$$\Psi : \mathbb{F}_p[\mathbb{T}][Y]/(G_0(Y)) \cong \mathbb{F}_p[x]/(\Phi_r(x))$$

is an $\mathbb{F}_p$-algebra isomorphism.

Example: Referring to the example on p.20 with $p = 31$, $r = 19$, $d = 6$, $m = 3$ and noting that $\alpha = 2$ is a primitive element of $\mathbb{F}_r$ we have

$$\begin{aligned} G_0(Y) &= Y^6 - T_0Y^5 + (3 + T_0 + T_2)Y^4 - (2 + 2T_0 + T_1)Y^3 \\ &\quad +(3 + T_0 + T_2)Y^2 - T_0Y + 1 \\ G_1(Y) &= Y^6 - T_1Y^5 + (3 + T_1 + T_0)Y^4 - (2 + 2T_1 + T_2)Y^3 \\ &\quad +(3 + T_1 + T_0)Y^2 - T_1Y + 1 \\ G_3(Y) &= Y^6 - T_2Y^5 + (3 + T_2 + T_1)Y^4 - (2 + 2T_2 + T_0)Y^3 \\ &\quad +(3 + T_2 + T_1)Y^2 - T_2Y + 1. \end{aligned} \tag{3.58}$$

Replacing Y by x and mapping

$$\begin{aligned} T_0 &\mapsto x + x^{12} + x^{11} + x^{18} + x^7 + x^8 \\ T_1 &\mapsto x^2 + x^5 + x^3 + x^{17} + x^{14} + x^{16} \\ T_2 &\mapsto x^4 + x^{10} + x^6 + x^{15} + x^9 + x^{13} \end{aligned} \tag{3.59}$$

and reducing the results mod Φ_{19} we get that

$$\begin{aligned} G_0(Y) &\mapsto 0 \\ G_1(Y) &\mapsto -1 + 3x^2 - 2x^3 + 3x^4 - x^6 - 3x^8 + x^9 \\ &\quad +x^{11} + x^{14} + x^{16} - 3x^{17} \\ G_2(Y) &\mapsto 4 + x + 4x^2 - x^3 + 4x^4 + x^5 + 4x^6 + 3x^8 \\ &\quad -x^9 - x^{11} - x^{14} - x^{16} + 3x^{17}. \end{aligned} \tag{3.60}$$

We know that the image of $G_1(Y)$ is congruent to $g_1 \bmod g_0$, $g_2 \bmod g_1$ and $g_0 \bmod g_2$. The image of $G_2(Y)$ is congruent to $g_2 \bmod g_0$, $g_0 \bmod g_1$ and $g_1 \bmod g_2$. ■

Chapter 4

Some Linear Algebra

In this chapter we describe some of the maps discussed in Chapter 3 as matrices and use the results to settle the uniqueness of the $\delta_{ij}^{(u)}$. We also describe a way to reduce the problem of deterministically factoring $\Phi_r(x)$ in time $r^{O(1)}$ to that of factoring a polynomial all of whose roots lie in $\mathbb{F}_p$. Finally, we construct a matrix representation of $\mathbb{F}_p[\mathbb{T}]$ and examine its generators to make some observations about the cyclotomic numbers.

4.1 $\varphi\psi$ as a matrix and the uniqueness of the $\delta_{ij}^{(u)}$

In this section we describe and examine the matrix for $\varphi\psi$ as a linear transformation and show that the $\delta_{ij}^{(u)}$ described in Section 2.2 are unique.

First recall, from (3.10), that there exists an $\mathbb{F}_p$-algebra homomorphism, $\varphi\psi : \mathbb{F}_p[\mathbb{T}] \to \mathbb{F}_p[x]/g_0[x] \oplus \cdots \oplus \mathbb{F}_p[x]/g_{m-1}(x)$, given by

$$\begin{aligned} T_0 &\mapsto (t_0, t_1, \cdots, t_{m-1}) \\ T_1 &\mapsto (t_1, t_2, \cdots, t_{m-1}, t_0) \\ &\vdots \\ T_i &\mapsto (t_i, t_{i+1}, \cdots, t_{i-1}) \\ &\vdots \\ T_{m-1} &\mapsto (t_{m-1}, t_0, \cdots, t_{m-2}). \end{aligned} \tag{4.1}$$

Noting that $\{T_0, \cdots, T_{m-1}\}$ is a basis for $\mathbb{F}_p[\mathbb{T}]$ over $\mathbb{F}_p$ and using $\{e_0, e_1, \cdots, e_{m-1}\}$, where $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ where the 1 is in the i^{th} position, as a basis for $\mathbb{F}_p[x]/g_0[x] \oplus \cdots \oplus \mathbb{F}_p[x]/g_{m-1}(x)$ over $\mathbb{F}_p$, we see that we may describe the $\mathbb{F}_p$-algebra homomorphism $\varphi\psi$ via the matrix

$$\begin{bmatrix} t_0 & t_1 & t_2 & \cdots & t_{m-1} \\ t_1 & t_2 & t_3 & \cdots & t_0 \\ & & \vdots & & \\ t_i & t_{i+1} & t_{i+2} & \cdots & t_{i-1} \\ & & \vdots & & \\ t_{m-1} & t_0 & t_1 & \cdots & t_{m-2} \end{bmatrix} \tag{4.2}$$

Several remarks about the matrix above. First, since $\varphi\psi$ is injective, in fact an isomorphism from $\mathbb{F}_p[\mathbb{T}]$ to $\mathcal{B}$, it follows that the matrix is non-singular, so has a non-zero determinant. Secondly, a matrix of this form, where each row is a shift one step left of the previous row, is called left circulant. We shall refer to it here as

lcirc$[t_0, \cdots, t_{m-1}]$. Note that by reversing the order of the rows, or simply reversing the order of one of the bases being used, we will get a matrix in which each row is a one step shift to the right of the previous row, known as a circulant matrix and referred to as circ$[t_0, \cdots, t_{m-1}]$. As the determinant of this matrix will differ from that of lcirc$[t_0, \cdots, t_{m-1}]$ by at most a factor of -1 it follows that it is non-singular as well.

There is a well known result[1] which states that circ$[a_0, \cdots, a_{m-1}]$ with entries in a finite field K, is non-singular if, and only if, the polynomial $a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}$ is relatively prime to the polynomial $x^m - 1$ over K. Noting that switching columns in any fashion does not affect the non-singularity of the matrix we have proved

Lemma 15 *The polynomial*

$$a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}$$

where $\{a_0, \cdots, a_{m-1}\} = \{t_0, \cdots, t_{m-1}\}$, *is relatively prime to* $x^m - 1$ *over* $\mathbb{F}_p$.

Back in Theorem 2 we demonstrated a technique for writing the coefficients of the $g_u(x)$ in a particular way as $\mathbb{F}_p$-linear combinations of the t_i. In particular, we noted that we could find a set of elements of $\mathbb{F}_p$, $\left\{\delta_{si}^{(u)}\right\}_{\substack{i,u \in \mathbb{Z}/m\mathbb{Z} \\ s \in \mathbb{Z}/d\mathbb{Z}}}$ so that the coefficient of x^s in $g_u(x)$ is

$$(-1)^{d-s} \sum_{i=0}^{m-1} \delta_{si}^{(u)} t_i. \tag{4.3}$$

We further saw that the $\delta_{si}^{(u)}$ satisfied the relations in (2.27). In particular, we had

[1] See, for example, Section 1.7 of [SMA]

$\delta_{st}^{(u+k)} = \delta_{s,t-k}^{(u)}$. That is, if the coefficient of x^s in $g_u(x)$ is

$$\delta_{s0}^{(u)} t_0 + \delta_{s1}^{(u)} t_1 + \cdots + \delta_{s,m-1}^{(u)} t_{m-1} \tag{4.4}$$

then the coefficient of x^s in $g_{u+k}(x)$ is

$$\begin{aligned} & \delta_{s0}^{(u+k)} t_0 + \delta_{s1}^{(u+k)} t_1 + \cdots + \delta_{s,m-1}^{(u+k)} t_{m-1} \\ = \; & \delta_{s,m-k}^{(u)} t_0 + \delta_{s,m-k+1}^{(u)} t_1 + \cdots + \delta_{s,m-k-1}^{(u)} t_{m-1} \\ = \; & \delta_{s0}^{(u)} t_k + \delta_{s1}^{(u)} t_{k+1} + \cdots + \delta_{s,m-1}^{(u)} t_{k-1}. \end{aligned} \tag{4.5}$$

If we now suppose that

$$g_u(x) = \alpha_{0u} + \alpha_{1u} x + \cdots + \alpha_{du} x^d \tag{4.6}$$

then we see that the $\delta_{si}^{(u)}$ must satisfy

$$\begin{bmatrix} t_0 & t_1 & t_2 & \cdots & t_{m-1} \\ t_1 & t_2 & t_3 & \cdots & t_0 \\ & & \vdots & & \\ t_i & t_{i+1} & t_{i+2} & \cdots & t_{i-1} \\ & & \vdots & & \\ t_{m-1} & t_0 & t_1 & \cdots & t_{m-2} \end{bmatrix} \begin{bmatrix} \delta_{s0}^{(u)} \\ \delta_{s1}^{(u)} \\ \vdots \\ \delta_{si}^{(u)} \\ \vdots \\ \delta_{s,m-1}^{(u)} \end{bmatrix} = \begin{bmatrix} \alpha_{su} \\ \alpha_{s,u+1} \\ \vdots \\ \alpha_{s,u+i} \\ \vdots \\ \alpha_{s,u+m-1} \end{bmatrix} \tag{4.7}$$

for each choice of $s \in \mathbb{Z}/d\mathbb{Z}$ and $u \in \mathbb{Z}/m\mathbb{Z}$. Since the matrix on the left is not singular it follows that the $\delta_{si}^{(u)}$ must be unique.

Recalling (2.27) we also see that all but $md = r - 1$ of the are $\delta_{si}^{(u)}$ redundant. If we define $\delta_{st} = \delta_{st}^{(0)}$ then we may write that the coefficient of x^s in $g_u(x)$ is

$$(-1)^{d-s} \sum_{i=0}^{m-1} \delta_{s,i-u} t_i \tag{4.8}$$

Hence we have proved the following version of Theorem 2.

Theorem 4 *There exist unique elements of* $\mathbb{F}_p$, $\{\delta_{st}\}_{\substack{t \in \mathbb{Z}/m\mathbb{Z} \\ s \in \mathbb{Z}/d\mathbb{Z}}}$, *that can be computed deterministically in time* $(r \log\ p)^{O(1)}$, *so that*

$$g_u(x) = \sum_{s=0}^{d} \left[(-1)^{d-s} \sum_{i=0}^{m-1} \delta_{s,i-u} t_i \right] x^s. \tag{4.9}$$

As in Theorem 2 we make two remarks. The first is that the number of operations required to compute the δ_{si} is $O(r^3 \log p)$ or, in the case where $p \gg r$, in particular, $p > 2^d$, $O(r^4)$ operations. Secondly, recall that $\delta_{st} \equiv \alpha_{st}^{(0)} - \beta_{st}^{(0)} \bmod p$, where $\alpha_{st}^{(0)}$ and $\beta_{st}^{(0)}$ were integers whose computations nowhere involved p and which were bounded by 2^d. So, if $p \gg r$, in particular, if $p > 2^d$, and we agree to represent δ_{st} as a negative if $\alpha_{st}^{(0)} < \beta_{st}^{(0)}$, then it follows that if p_1 and p_2 are primes with $\mathrm{ord}(p_1, r) = \mathrm{ord}(p_2, r)$, then the δ_{st} will be the same whether we are working over $\mathbb{F}_{p_1}$ or $\mathbb{F}_{p_2}$.

4.2 A reduction to factoring a polynomial which splits

In this section we show that finding the traces of the irreducible factors of $\Phi_r(x)$ can be reduced in time $r^{O(1)}$ to that of factoring a specific polynomial which splits over $\mathbb{F}_p$.

Recalling that $\mathbb{F}_p[\mathbb{T}]$ is an m-dimensional $\mathbb{F}_p$-vector space it follows that $1, T_0, T_0^2, \cdots, T_0^m$ form a linearly dependent set in $\mathbb{F}_p[\mathbb{T}]$ over $\mathbb{F}_p$, so there exists $\alpha_0, \alpha_1, \cdots, \alpha_m \in \mathbb{F}_p$, not all zero, such that

$$\alpha_0 + \alpha_1 T_0 + \alpha_2 T_0^2 + \cdots + \alpha_m T_0^m = 0 \in \mathbb{F}_p[\mathbb{T}]. \tag{4.10}$$

Note that by expressing $T_0^2, \cdots, T_0^m$ as linear combinations of the basis $T_0, T_1, \cdots, T_{m-1}$ we may compute $\alpha_0, \alpha_1, \cdots, \alpha_m$ in time polynomial in r and $\log p$ by performing Gaussian elimination on an $(m+1) \times m$ matrix with entries in $\mathbb{F}_p$.

Recalling the shift automorphism, σ, it follows that for $i = 1, \cdots, m$ we have

$$\begin{aligned} & \sigma^i \left(\alpha_0 + \alpha_1 T_0 + \alpha_2 T_0^2 + \cdots + \alpha_m T_0^m \right) \qquad (4.11) \\ = \;& \alpha_0 + \alpha_1 T_i + \alpha_2 T_i^2 + \cdots + \alpha_m T_i^m = 0. \end{aligned}$$

That is, working in $\mathbb{F}_p[\mathbb{T}][Y]$ over $\mathbb{F}_p[\mathbb{T}]$, $T_0, T_1, \cdots, T_{m-1}$ are all roots of the polynomial

$$h(y) = \alpha_0 + \alpha_1 Y + \alpha_2 Y^2 + \cdots + \alpha_m Y^m \tag{4.12}$$

in $\mathbb{F}_p[\mathbb{T}][Y]$.

Now note that the image of $\alpha_0 + \alpha_1 T_0 + \alpha_2 T_0^2 + \cdots + \alpha_m T_0^m$ under $\varphi\psi$ is the m-tuple whose i^{th} component is

$$h(t_i) = \alpha_0 + \alpha_1 t_i + \alpha_2 t_i^2 + \cdots + \alpha_m t_i^m. \tag{4.13}$$

Referring to (4.11) we see that we must have that

$$h(t_i) = \alpha_0 + \alpha_1 t_i + \alpha_2 t_i^2 + \cdots + \alpha_m t_i^m = 0 \tag{4.14}$$

for all $i \in \mathbb{Z}/m\mathbb{Z}$. Therefore, working in $\mathbb{F}_p[x]$ over $\mathbb{F}_p$, we have that $t_0, t_1, \cdots, t_{m-1}$ must be precisely the roots of $h(x)$ over $\mathbb{F}_p$. That is, multiplying by a suitable constant if necessary,

$$h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_m x^m = \prod_{i=0}^{m-1} (x - t_i) \tag{4.15}$$

is a polynomial with coefficients in $\mathbb{F}_p$ which splits over $\mathbb{F}_p$. If we could factor this polynomial then we would know all of the t_i and could therefore completely factor $\Phi_r(x)$ over $\mathbb{F}_p$ using either the techniques of Chapter 2 or of Chapter 3. Hence we have proved

Lemma 16 *The problem of deterministically factoring Φ_r over $\mathbb{F}_p$ can be reduced, in time $(r \log\ p)^{O(1)}$ to that of factoring an m^{th} degree polynomial over $\mathbb{F}_p$, which splits in $\mathbb{F}_p$.*

It should also be noted that by formally expanding the right hand side of (4.15) it follows that

$$\sum t_{i_1} t_{i_2} \cdots t_{i_k} = (-1)^k \alpha_{m-k} \tag{4.16}$$

where the sum is over all k-element subsets of $\{0, 1, \cdots, m-1\}$. In particular

$$t_0 t_1 \cdots t_{m-1} = \alpha_0. \tag{4.17}$$

Example: As in the example on page 20, let $p = 31$, r=19, hence $d = 6$, $m = 3$, and choosing $\alpha = 2$, we find the cyclotomic numbers $(0,0) = 2$, $(0,1) = 1$, and $(0,2) = 2$. Then using the relations in (3.3) we find that

$$T_0^2 = -4T_0 - 5T_1 - 4T_2 \tag{4.18}$$

$$T_0^3 = 3T_0 - 2T_1 - 3T_2$$

and using $1 = -T_0 - T_1 - T_2$ we get the matrix

$$\begin{bmatrix} -1 & 1 & -4 & 3 & 0 \\ -1 & 0 & -5 & -2 & 0 \\ -1 & 0 & -4 & -3 & 0 \end{bmatrix} \tag{4.19}$$

Performing Gaussian elimination over $\mathbb{Z}$ and setting $\alpha_3 = 1$ we get the solution $\alpha_0 = -7$, $\alpha_1 = -6$, $\alpha_2 = 1$ and $\alpha_3 = 1$. Hence

$$h(x) = x^3 + x^2 - 6x - 7 \tag{4.20}$$

from which we observe that it must be the case that

$$t_0 t_1 t_2 = 7$$

and that

$$t_0 t_1 + t_0 t_2 + t_1 t_2 = -6$$

Please note that the above formulas, as well as $h(x)$, will be the same over $\mathbb{F}_p$ with $r = 19$ as long as the $\text{ord}(p, 19) = 6$. If we further factor $h(x)$ over $\mathbb{F}_{31}$ as

$$h(x) = (x + 12)(x + 4)(x + 16) \tag{4.21}$$

then we see that the traces of the irreducible factors of Φ_{19} are 19, 27 and 15. Using the techniques outlined in either Chapters 2 or 3 we could now factor $\Phi_{19}(x)$. ■

4.3 Matrix representation

In this section we construct the left-regular matrix representation of $\mathbb{F}_p[\mathbb{T}]$ in $\mathbb{M}_m(\mathbb{F}_p)$, the ring of $m \times m$ matrices with entries in $\mathbb{F}_p$ and examine some of the characteristics of these matrices.

Using $\{T_0, T_1, \cdots, T_{m-1}\}$ as an $\mathbb{F}_p$-basis for $\mathbb{F}_p[\mathbb{T}]$ we let $M^{(k)}$ be the $m \times m$ matrix whose ij^{th} entry is the coefficient of T_j in the expansion of $T_k T_i$ [for convenience we shall number the rows and columns of the matrices by $0, 1, \cdots, m-1$]. Recalling the formula (1.9) and referring to the ij^{th} entry of $M^{(k)}$ as $m_{ij}^{(k)}$, we have

$$m_{ij}^{(k)} = (i-k, j-k) - d\theta_{i-k} \tag{4.22}$$

where $(i-k, j-k)$ refers to the appropriate cyclotomic number and θ_{i-k} is as defined in Lemma 1. The $\mathbb{F}_p$-subalgebra of $\mathbb{M}_m(\mathbb{F}_p)$ generated by the matrices $M^{(0)}$, $M^{(1)}$, $\cdots$, $M^{(m-1)}$ will now serve as a matrix representation of $\mathbb{F}_p[\mathbb{T}]$. If we let $f : \mathbb{F}_p[\mathbb{T}] \rightarrow \mathbb{M}_m(\mathbb{F}_p)$ be the linear transformation defined by $f : T_i \mapsto M^{(i)}$, then f is the $\mathbb{F}_p$-algebra isomorphism from $\mathbb{F}_p[\mathbb{T}]$ onto this representation.

Example: As in the example on page 20, let $p = 31$, $r = 19$, hence $m = 3$, $d = 6$, and choose $\alpha = 2$. We easily compute the 3×3 matrix whose ij^{th} entry is the

cyclotomic number (i, j) to be

$$\begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \tag{4.23}$$

and so we get

$$M^{(0)} = \begin{pmatrix} -4 & -5 & -4 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$M^{(1)} = \begin{pmatrix} 1 & 2 & 3 \\ -4 & -4 & -5 \\ 3 & 1 & 2 \end{pmatrix} \tag{4.24}$$

$$M^{(2)} = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ -5 & -4 & -4 \end{pmatrix}$$

and these generate the matrix representation of $\mathbb{F}_{31}[\mathbb{T}]$. It should be noted that these generators are completely independent of the characteristic of the field. That is, if p is any prime so that the ord$(p, 19)$ is 6, then we will get precisely the same generators for the matrix representation of $\mathbb{F}_p[\mathbb{T}]$. ■

Note also that we have

$$\begin{aligned} m_{i+1,j+1}^{(k+1)} &= (i+1-(k+1), j+1-(k+1)) - d\theta_{i+1-(k+1)} \\ &= (i-k, j-k) - d\theta_{i-k} \\ &= m_{ij}^{(k)}. \end{aligned} \tag{4.25}$$

That is, we can get $M^{(k+1)}$ from $M^{(k)}$ by shifting all rows down by one and all columns to the right by one. If we let U be the matrix whose ij^{th} entry is $\delta_{i,j-1}$(Kronecker's delta) then left multiplication by U shifts all rows down by one and right multiplication by $U^{-1} = U^t$ shifts all columns to the right by one. Recalling the $\mathbb{F}_p[\mathbb{T}]$-automorphism τ from (3.43) we see that

$$\tau(\lambda) = U f(\lambda) U^t \tag{4.26}$$

for any $\lambda \in \mathbb{F}_p[\mathbb{T}]$. In particular, note that for each i

$$M^{(i)} = U^i M^{(0)} \left(U^{-1}\right)^i \tag{4.27}$$

from which it follows that each of the $M^{(i)}$ have the same determinant. We should also note that since each of the $M^{(i)}$ have the same numbers on the main diagonal they must also all have the same trace. We also observe that each of the $M^{(i)}$ must satisfy the polynomial $h(x)$ referred to in (4.15), hence it follows that

$$\text{charpoly}\left(M^{(i)}\right) = h(x) = \prod_{i=0}^{m-1} (x - t_i). \tag{4.28}$$

Noting that the trace of $h(x)$ is -1 we have proved the following result regarding cyclotomic numbers.

Corollary 5

$$\sum_{i=0}^{m-1}(i,i) = d-1.$$

Using the basic identities on the cyclotomic numbers from Lemma 1 we now note that the sum of the entries in the i^{th} row of $M^{(0)}$ is

$$\begin{aligned}
\sum_{j=0}^{m-1} m_{ij}^{(0)} &= \sum_{j=0}^{m-1}[(i,j) - d\theta_i] \\
&= \left[\sum_{j=0}^{m-1}(i,j)\right] - md\theta_i \qquad (4.29) \\
&= d - \theta_i - md\theta_i \\
&= \begin{cases} d-r, & d \text{ even}, i=0 \\ d-r & d \text{ odd}, i=\frac{m}{2} \\ d & \text{otherwise} \end{cases}.
\end{aligned}$$

Similarly, the sum of the entries in the j^{th} column of $M^{(0)}$ is

$$\begin{aligned}
\sum_{i=0}^{m-1} m_{ij}^{(0)} &= \sum_{i=0}^{m-1}[(i,j) - d\theta_i] \\
&= \left[\sum_{j=0}^{m-1}(i,j)\right] - d \qquad (4.30) \\
&= d - \eta_j - d \\
&= \begin{cases} -1, & \text{if } j=0 \\ 0 & \text{otherwise} \end{cases}.
\end{aligned}$$

In so much as elementary symmetric forms, in particular, sums of the form

$$\sum_{i=0}^{m-1} T_i^k \qquad (4.31)$$

may be of interest, we note that, of course, $\sum_{i=0}^{m-1} T_i^0 = m$ and $\sum_{i=0}^{m-1} T_i = -1$. In the case $k = 2$, note that row 0 of $M^{(0)}$ consists of the coefficients of T_0^2. Suppose that this row is $[r_0\ r_1\ \cdots\ r_{m-1}]$, then shifting to the left by i yields $[r_i\ r_{i+1}\ \cdots\ r_{i-1}]$ hence

$$\begin{aligned} \sum_{i=0}^{m-1} T_i^2 &= \sum_{i=0}^{m-1} r_i (T_0 + T_1 + \cdots T_{m-1}) \\ &= -\sum_{i=0}^{m-1} r_i \\ &= \begin{cases} r - d, & d \text{ even} \\ -d & d \text{ odd} \end{cases} \end{aligned} \tag{4.32}$$

by (4.29). Looking at $\varphi\psi\left(\sum_{i=0}^{m-1} T_i^2\right)$ it follows that we also have

$$\sum_{i=0}^{m-1} t_i^2 = \begin{cases} r - d, & d \text{ even} \\ -d & d \text{ odd} \end{cases}$$

in $\mathbb{F}_p$.

REFERENCES

BIN D. Bini and V. Pan, **Polynomial and Matrix Computations**, Birkhauser, Boston, (1994).

BAU L.D. Baumert and W.H. Mills, *Uniform cyclotomy*, Journal of Number Theory, [**14**], (1982), 67-82.

COH H. Cohen, **A Course in Computational Algebraic Number Theory**, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, (1995).

CUR C. Curtis and I. Reiner, **Representation Theory of Finite Groups and Associative Algebras**, Interscience, New York, (1962).

DAV R. Davis, *Idempotent computation over finite fields*, J. Symbolic Computation, [**17**], (1994), 237-258.

DIC L.E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., [**57**], (1935), 391-424.

GAT J. von zur Gathen and V. Shoup, *Computing Frobenius maps and factoring polynomials,* Comput. Complexity, [**2**], (1992), 187-224.

JAC N. Jacobson, **Basic Algebra**, vols. I and II, W.H. Freeman, San Francisco, (1980).

JUN D. Jungnickel, **Finite Fields**, Wissenschaftsverlag, Mannheim, (1993).

KNU D. Knuth, **The Art of Computer Programming**, volume 2, *Semi-numerical algorithms,* 2nd ed.,Addison-Wesley, Reading, (1981).

LAN S. Lang, **Algebra**, 2^{nd} ed.,Addison-Wesley, Reading, (1984).

LEN H. W. Lenstra, Jr., *Finding isomorphims between finite fields*, Math. Comp., [**56**], (1991), 329-347.

LID1 R. Lidl and H. Niederreiter, **Finite Fields**, Encyclopedia of Mathematics and its Applications, v. 20, Addison-Wesley, Reading, 1983.

LID2 R. Lidl and H. Niederreiter, **Introduction to Finite Fields and their Applications**, revised edition, Cambridge University Press, Cambridge, 1994.

MEN A. J. Menezes, ed., **Applications of Finite Fields**, Kluwer, Boston, (1993).

MYE G. Myerson, *Period polynomials and Gauss sums for finite fields*, Acta Arith., [**39**], (1981), 251-264.

NIE1 H. Niederreiter and R. Gottfert, *Factorization of polynomials over finite fields and characteristic sequences*, J. Symbolic Computation, [**16**], (1993), 401-412.

NIE2 H. Niederreiter and R. Gottfert, *On a new factorization algorithm for polynomials over finite fields*, (preprint).

SCH R. Schoof, *Elliptic curves over finite fields and the computation of square roots* mod p, Math. Comp. [**44**], (1985), pp. 483-494.

SHO V. Shoup, *New algorithms for finding irreducible polynomials over finite fields,* Math. Comp. [**54**], (1990), pp. 435-447.

SMA C. Small, **Arithmetic of Finite Fields**, Marcel Dekker, New York, (1991).

STE G. Stein, *Factoring cyclotomic polynomials over large finite fields,* **Finite Fields and Applications**, London Mathematical Society Lecture Note Series #233, S. Cohen & R. Niederrieter, eds., Cambridge University Press, pp. 349-354 (1996).

STO T. Storer, **Cyclotomy and Difference Sets**, Markham, Chicago, 1967.