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

Construction Of The Orthogonal Groups Of $n \times n$ Circulant Matrices Over Finite Fields

Zhe Zhang

A Thesis

in

The Department

of

Mathematics & Statistics

Presented in Partial Fulfillment of the Requirements

for the degree of Master of Science at

Concordia University

Montreal, Quebec, Canada

January 1997

Abstract

Construction Of The Orthogonal Groups Of $n \times n$ Circulant Matrices Over Finite Fields

Zhe Zhang

Let F be a finite field with q elements where $q = p^m$, p prime. Let $\mathcal{M}$ be the algebra of $n \times n$ circulant matrices over F. The set $O_{(n,q)}$ of orthogonal $n \times n$ circulant matrices is a subgroup of $\mathcal{M}^\times$. The major purposes of the thesis are: (1) to explain K.A.Byrd and T.P. Vaughan's results stated in [8], about formulas for the orders, and algorithms for the construction, of the groups $O_{(n,q)}$; (2) to show new examples and develop programs to find the orders and to actually construct the group $O_{(n,q)}$ for any given n and q.

ACKNOWLEDGMENTS

The author is indebted to his teacher and supervisor, Professor F. Thaine, for his help and advice during the preparation of this thesis. The author also thanks Professor Jesus Gomez Ayala from the Universidad del Pais Vasco for his important suggestion about this thesis.

TABLE OF CONTENTS

Introduction 1

Chapter 1. Review of Field Extensions and Finite Fields 4

Chapter 2. Orthogonal Circulant Matrices over Finite Fields 17

Chapter 3. Construction of The Orthogonal Circulant Matrix Groups $O_{(12,3)}$, $O_{(6,2)}$ and $O_{(14,2)}$ 49

Chapter 4. Normal and Normal orthogonal Bases over Finite Fields 64

Chapter 5. The Program for Constructing The Orthogonal Group of $O_{(n,q)}$ 72

References 77

Appendix. Source code of the program

Introduction

The objects of study in this thesis are the circulant orthogonal matrices over finite fields, and the related normal orthogonal basis for extensions of finite fields. Let p be a prime number, and m and n positive integers, call F the Galois field $GF(q)$, where $q = p^m$. Our main purpose is to develop some formulas to count the orders of the circulant orthogonal matrix groups $O_{(n,q)}$ of order n over F, and algorithms to construct such matrices. Recall that a circulant matrix of order n over F is a matrix

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

with $a_i \in F$, and also that an $n \times n$ matrix A is orthogonal if $A \cdot A^t = I$. The formulas mentioned above have first been obtained by F.J. MacWilliams [7]. Here we use a new method due to K.A. Byrd and T.P. Vaughan to obtain these formulas and to actually construct the matrices. As an extension, we use the Maple [13] system to develop a program to construct the circulant orthogonal matrix groups $O_{(n,q)}$ for any given n and $q = p^m$. The program requires the parameters n, p and m as input and calculates the elements of the group $O_{(n,q)}$.

In Chapter 1 we review some basic concepts of the theory of finite fields and field extensions. In Chapter 2, we explain Byrd and Vaughan's results as stated in [8], and we take the liberty to expand some of their proofs. Let T be the $n \times n$ circulant matrix with first row $(0, 1, 0, \cdots, 0)$. Since $T^n = I$, and any circulant matrix A as above can been written in the form $A = a_0 \cdot I + a_1 \cdot T + \cdots + a_{n-1} \cdot T^{n-1}$, we can construct an isomorphism φ from the ring $\mathcal{M}$ of $n \times n$ circulant matrices over F to

the ring $R_n = F[x]/(x^n - 1)$ by defining $\varphi(T) = x$ and $\varphi(a) = a$ for all $a \in F$. This isomorphism induces a transpose map τ on R_n corresponding to the transpose map of matrices. Call $\mathcal{O}$ the orthogonal group of R_n (that is the set $\{f \in R_n : f \cdot \tau(f) = 1\}$). Since $O_{(n,q)}$ is isomorphic to $\mathcal{O}$, we can concentrate on the study this later group. This allows us to work with polynomials. Write $x^n - 1$ as product of monic irreducible polynomials f_i; that is $x^n - 1 = f_1^{n_1} \cdot f_2^{n_2} \cdots f_r^{n_r}$. Then, by the Chinese remainder, theorem we have $R_n \cong \frac{F[x]}{(f_1^{n_1})} \times \frac{F[x]}{(f_2^{n_2})} \times \cdots \times \frac{F[x]}{(f_r^{n_r})}$. Equivalently we can write $R_n \cong \bigoplus_{i=1}^{r} e_i R_n$, where the e_i are certain elements of R_n (idempontents) satisfying $e_i^2 = e_i$, $e_i e_j = 0$ if $i \neq j$ and $e_i R_n \cong F[x]/(f_i^{n_i})$ (see Chapter 2, Theorem 3.5). The transpose map τ is an automorphism of R_n that can be defined by $\tau(x) = x^{-1}$ and $\tau(a) = a$ for all $a \in F$. When we restrict this map to components $e_i R_n$, $1 \leq i \leq r$, two cases arise: (i) $\tau(e_i) = e_i$, or (ii) $\tau(e_i) = e_j$ for some $j \neq i$. If $\tau(e_i) = e_i$, the effect of τ is to produce an automorphism of $F[x]/(f_i^{n_i})$. If $\tau(e_i) = e_j$ for $i \neq j$, the effect of τ is to produce an isomorphism from $F[x]/(f_i^{n_i})$ to $F[x]/(f_j^{n_j})$. In case (i) let $\mathcal{O}_i$ denote the orthogonal group of $F[x]/(f_i^{n_i})$ and in case (ii) let $\mathcal{O}_{(i,j)}$ denote the orthogonal group of $F[x]/(f_i^{n_i}) \times F[x]/(f_j^{n_j})$. Then we have $\mathcal{O} \cong \Pi_i \mathcal{O}_i \times \Pi_{(k,l)} \mathcal{O}_{(k,l)}$, where i runs through all indices i such that $\tau(e_i) = e_i$ and (k,l) runs through all pairs of indices $\{k,l\}$, $k \neq l$ such that $\tau(e_k) = e_l$. Hence to find the order $|\mathcal{O}|$ it is enough to find the orders $|\mathcal{O}_i|$ and $|\mathcal{O}_{(k,l)}|$. The study of the groups $\mathcal{O}_i$ and $\mathcal{O}_{(k,l)}$ is done in the sections "1-cycle case" and "2-cycle case" of Chapter 2.

As new examples of application of the method, we give, in Chapter 3, the detailed construction of the groups $O_{(12,3)}$ of 12×12 circulant orthogonal matrices over

$F = GF(3)$ and $O_{(6,2)}$ of 6×6 circulant orthogonal matrices over $F = GF(2)$. Though these problems are easy to calculate by using the program given in Chapter 5, in this chapter we show the mathematical ideas involved in constructing such groups.

In Chapter 4, we study normal orthogonal basis for extensions of finite fields. We show that the transformation matrix between any two such basis, if they exist (see Theorem 3.3), is circulant orthogonal, and conversely given a normal orthogonal basis for an extension of degree n, and a $n \times n$ circulant orthogonal matrix, we obtain another normal orthogonal basis by using the transformation induced by the matrix. This shows that the results of Chapter 2 can be used to find all normal orthogonal basis for a field extension when one of them is known.

Finally we show, in Chapter 5, a program to construct the group $O_{(n,q)}$ given arbitrary n and $q = p^m$.

Chapter 1. Review of Field Extensions and Finite fields.

If K is a field containing a field F, then K is said to be an extension field of F. In such case we write K/F. Here we are mainly interested in extensions of finite fields. Let K be an extension of F and let D be a subset of K. We denote by $F(D)$ the smallest subfield of K which contains both F and D; this is the intersection of all the subfields of K which contain both F and D. The field $F(D)$ is an extension of E.

One of the main invariants associated with a field F is its characteristic. Let 1_F denote the identity element of the field F. Then F contains the elements $1_F, 1_F + 1_F, \cdots$ of the additive subgroup of F generated by 1_F , which may not all be distinct. For any positive integer n, let $n \cdot 1_F = 1_F + 1_F + \cdots + 1_F (n \text{ times})$. Then either $n \cdot 1_F = 0$ for some $n > 0$ or all the elements $n \cdot 1_F$ are distinct. In the first case we find that the smallest positive integer n such that $n \cdot 1_F = 0$ is a prime number p. In this case we say that the field F has characteristic p. Otherwise we say that the field F has characteristic 0. Clearly a finite field must have characteristic p for some prime p.

Any field F contains as a subfield the field generated by 1_F. We call this subfield the **prime subfield** of F. If the characteristic of F is p, the prime subfield of F is F_p the field with p elements. If the characteristic of F is 0, the prime subfield of F is isomorphisc to $\mathbb{Q}$. We denote the characteristic of F by $\operatorname{Char} F$. If $\operatorname{Char} F = p$ (p a prime number), the map $\alpha \mapsto \alpha^p$ from F to F is called the **Frobenius** map of F.

THEOREM 1.1. *If F is a field with $CharF = p$, then Frobenius map of F is an injective endomorphism.*

PROOF. Since for every $\alpha \in F$ if $\alpha^p = 0$ then $\alpha = 0$, we need only to prove that the Frobenius map of F is an endomorphism. Since $(\alpha\beta)^p = \alpha^p\beta^p$, it suffices to verify that

$$(\alpha + \beta)^p = \alpha^p + \beta^p \quad \forall \alpha, \beta \in F$$

Let $1 \leq k \leq p-1$. Since

$$p \nmid k!, \quad p \nmid (p-k)!, \quad p | p!,$$

and

$$p! = k!(p-k)!\binom{p}{k},$$

we have $p|\binom{p}{k}$. Hence $\binom{p}{k} = 0$ in F.

Therefore $(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k}\alpha^{p-k}\beta^k = \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k}\alpha^{p-k}\beta^k + \beta^p = \alpha^p + \beta^p$. □

We say that a field is **perfect** when either it has characteristic 0 or, it has prime characteristic p and its Forbenius map is an automorphism. If F is a field with Char$F = p$, let F^p denote the image of the Frobenius map of F. Then F^p is the subfield of F consisting of the elements of F that admit pth roots in F; and the map $\alpha \to \alpha^p$ from F to F^p is an isomorphism. It follows that a field F with Char$F = p$

is perfect if and only if $F^p = F$, hence if and only if every element of F admits a pth root in F. For finite fields we have the following proposition.

PROPOSITION 1.2. *If F is a finite field then F is perfect; i.e. the Frobenius map is an automorphism of F.*

PROOF. The injectivity of the Frobenius endomorphism of F implies that it is also surjective if F is finite. □

If D is a finite subset of an extension K of the field F, say $D = \{a_1, ..., a_n\}$, we will denote $F(D)$ by $F(a_1, ..., a_n)$. If K is an extension of F then it is a linear vector space over F. The dimension of this vector space is called the degree of K over F and is denoted by $[K : F]$. If $[K : F]$ is finite, we say that K is a **finite extension** of F, if $[K : F]$ is infinite we say that K is an **infinite extension** of K.

PROPOSITION 1.3. *Let F be a field, K an extension of F, and L an extension of K.*

(i) If $(\alpha_i)_{i\in I}$ and $(\beta_j)_{j\in J}$ are, respectively, linear bases of K over F and of L over K, then $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ is a linear base of L over F.

(ii) $[L : F] = [L : K][K : F]$

(iii) L is finite over F if and only if L is finite over K and K is finite over F.

PROOF. We need only to prove (i), since (i) implies (ii) and (iii). Let $(\alpha_i)_{i\in I}$ and $(\beta_j)_{j\in J}$ be as in (i), and let $l \in L$, then $l = \sum_{j\in J} a_j\beta_j$ with $a_j \in K$. Since

$(\alpha_i)_{i\in I}$ is a base of K over F, for every $j \in J$, we can write $a_j = \sum_{i\in I} b_{ij}\alpha_i$, where $b_{ij} \in F$. So we have

$$l = \sum_{j\in J} a_j\beta_j = \sum_{(i,j)\in I\times J} b_{ij}\alpha_i\beta_j$$

which shows that l is a linear combination of $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ with coefficients in F. Assume that

$$l = \sum_{j\in J} a_j\beta_j = \sum_{(i,j)\in I\times J} b_{ij}\alpha_i\beta_j = 0$$

with $b_{i,j} \in F$ and $a_j = \sum_{i\in I} b_{ij}\alpha_i$. Since $(\beta_j)_{j\in J}$ is a base of L over K, and $(b_{ij}\alpha_i) \in K$ for every $(i,j) \in I \times J$, we have $a_j = \sum_{i\in I} b_{ij}\alpha_i = 0$ for every $j \in J$; and the linear independence of $(\alpha_i)_{i\in I}$ over F implies then that $b_{ij} = 0$ for every $(i,j) \in I \times J$. Therefore $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ is linearly independent over F. □

If K is a finite extension of F and if $\alpha_1, ..., \alpha_n$ is a basis of K over F, then every element of K can be written in the form $\sum_{i=1}^{n} b_i\alpha_i$, $b_i \in F$ for $1 \leq i \leq n$. Since these sums are clearly in $F(\alpha_1, ..., \alpha_n)$ we have $K = F(\alpha_1, ..., \alpha_n)$. An extension K of F is called a simple extension of F if $K = F(\alpha)$ for some $\alpha \in K$.

DEFINITION. *Let $\alpha \in K$, we say that α is algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F then α is said to be transcendental over F. The extension field K of F is said to be an algebraic extension if each element of K is algebraic over F. On the other hand, if at least one element of K is transcendental over F, then K is called a transcendental extension of F.*

Suppose that $\alpha \in K$ is algebraic over F, let us consider the set $\mathcal{J} = \{f \in F[x] : f(\alpha) = 0\}$. It is obvious that $\mathcal{J}$ is an ideal of $F[x]$. Since α is algebraic over F, we have $\mathcal{J} \neq (0)$. Since $F[x]$ is a principal ideal domain, it follows that there exists a uniquely determined monic polynomial $p(\alpha, F)(x) \in F[x]$ such that $\mathcal{J}$ is equal to the pricipal ideal $(p(\alpha, F)(x))$. We have that $p(\alpha, F)(x)$ is irreducible in $F[x]$. In fact, $p(\alpha, F)(x)$ has positive degree since it has α as its root, and if $p(\alpha, F)(x) = h_1 h_2$ for some h_1, h_2 in $F[x]$ with $1 \leq \deg(h_i) < \deg(p(\alpha, F)(x))$ for $i = 1, 2$, then $p(\alpha, F)(\alpha) = h_1(\alpha)h_2(\alpha) = 0$ which implies that either h_1 or h_2 in $\mathcal{J}$ and so divisible by $p(\alpha, F)(x)$; it is impossible.

DEFINITION. *Let $\alpha \in K$ be algebraic over F, then the uniquely determined monic polynomial $p(\alpha, F)(x) \in F[x]$ generating the ideal $\mathcal{J} = \{f \in F[x] : f(\alpha) = 0\}$ of $F[x]$ is called the minimal polynomial of α over F. The degree of α over F is the degree of $p(\alpha, F)(x)$.*

THEOREM 1.4. *Let $\alpha \in K$ be algebraic over F, then its minimal polynomial $p(\alpha, F)(x)$ over F has the following properties:*

(i) $p(\alpha, F)(x)$ *is irreducible in* $F[x]$.

(ii) For $f \in F[x]$ *we have* $f(\alpha) = 0$ *if and only if* $p(\alpha, F)(x)$ *divides* f.

(iii) $p(\alpha, F)(x)$ *is the monic polynomial in* $F[x]$ *of least degree having* α *as a root.*

PROOF. (i) was already noted above. (ii) follows from the definition of $p(\alpha, F)(x)$. (iii) it suffices to note that any monic polynomial in $F[x]$ having α as a root must be a multiple of $p(\alpha, F)(x)$, and so it is either equal to $p(\alpha, F)(x)$ or its degree is larger than that of $p(\alpha, F)(x)$. □

COROLLARY 1.5. *If K/F is an extension of fields and α is algebraic over F (so it is also algebraic over K), then $p(\alpha, K)(x)$ divides $p(\alpha, F)(x)$ in $K[x]$.*

THEOREM 1.6. *Every finite extension of F is algebraic over F.*

PROOF. Suppose that K is an finite extension of F and let $n = [K : F]$. Then for $\alpha \in K$, the $n+1$ elements $1, \alpha, ..., \alpha^n$ must be linearly dependent over F. So we have $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ with $a_i \in F$ not all being 0, which means that α is algebraic over F. □

THEOREM 1.7. *Let $\alpha \in K$ be algebraic with degree n over F and let $p(\alpha, F)(x)$ be the minimal polynomial of α over F. Then we have*

(i) $F(\alpha) \cong F[x]/(p(\alpha, F)(x))$.

(ii) $[F(\alpha) : F] = n$ *and* $\{1, \alpha, ..., \alpha^{n-1}\}$ *is a basis of* $F(\alpha)$ *over* F.

(iii) Every $\beta \in F(\alpha)$ is algebraic over F and its degree over F is a divisor of n.

PROOF. (i) Let φ be the natural ring homomorphism of $F[x] \to F(\alpha)$, defined by $\varphi(f(x)) = f(\alpha)$ for $f \in F[x]$. Namely φ fixes the elements of F and sends x to α. Since $p(\alpha, F)(x)$ is the minimal polynomial of $F(\alpha)$, we have that the kernel of φ is the ideal generated by $p(\alpha, F)(x)$. Thus we have an induced injective ring homomorphism $\varphi' : F[x]/(p(\alpha, F)(x)) \to F(\alpha)$. In particular $F[x]/(p(\alpha, F)(x))$ is a domain. This gives another proof of the fact that $p(\alpha, F)(x)$ is irreducible. So $F[x]/(p(\alpha, F)(x))$ is a field, and, since the image of φ' is a field containing F and α we have that φ' is a field isomorphism from $F[x]/(p(\alpha, F)(x))$ to $F(\alpha)$.

(ii) By (i), we know that $F(\alpha)$ is the image of φ, so any given $\beta \in F(\alpha)$ can be written in the form $\beta = f(\alpha)$ for some $f(x) \in F[x]$. By the Euclidean Algorithm, we have $f(x) = q(x)p(\alpha, F)(x) + r(x)$ with $q, r \in F[x]$ and $r = 0$ or $\deg(r) < \deg(p(\alpha, F)(x)) = n$. So that $\beta = r(\alpha)$, i.e. β is a linear combination of $1, \alpha, ..., \alpha^{n-1}$ with coefficients in F. On the other hand, if $a_0 + a_1\alpha + \cdots + a_n\alpha^{n-1} = 0$ where $a_i \in F$, then $h(x) = a_0 + a_1x + \cdots + a_nx^{n-1} \in F[x]$ has α as a root. By Theorem 1.4 it is thus a multiple of $p(\alpha, F)(x)$. Since $h = 0$ or $\deg(h) < n = \deg(p(\alpha, F)(x))$, we have $h = 0$, that is, all a_i are zero. Therefore the elements $1, \alpha, ..., \alpha^{n-1}$ are linearly independent over F and (ii) follows.
(iii) By (ii), we have that $F(\alpha)$ is a finite extension of F, so for $\beta \in F(\alpha)$ is algebraic over F by Theorem 1.6. Furthermore, $F(\beta)$ is a subfield of $F(\alpha)$. If d is the degree of β over F, then (ii) and Proposition 1.3 imply that $n = [F(\alpha) : F] =$
$[F(\alpha) : F(\beta)][F(\beta) : F] = [F(\alpha) : F(\beta)]d$, hence d divides n. □

Let K be an extension of the field F, let $\alpha \in K$ and let $p(\alpha, F)(x)$ be the minimal polynomial of α over F. Suppose that β is root of $p(\alpha, F)(x)$, then $p(\alpha, F)(x)$ is also the minimal polynomial of β over F. By Theorem 1.7 (i), we have $F(\alpha) \cong F(\beta)$. This proves the following result.

THEOREM 1.8. *Let α and β be two roots of the polynomial $f \in F[x]$ that is irreducible over F. Then $F(\alpha)$ and $F(\beta)$ are isomorphic under the isomorphism mapping which sends α to β and fixes the elements of F.*

DEFINITION. *Let $f(x) \in F[x]$. Then $f(x)$ is said to split over F if $f(x)$ can be written as a product of linear factor in $F[x]$. The field K is a splitting field of*

$f(x)$ over F if $f(x)$ factors completely into factors in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

We say that the polynomial $f(x) \in F[x]$ is separable if it has no multiple roots over F. An extension field K of F is said to be separable over F if every element of K is the root of a separable polynomial over F. Let F be a field and let K be an extension field of F, we say that K is normal over F or that K is a normal extension of F if K is algebraic over F and the minimal polynomial over F of every element of K splits in $K[x]$. If K is normal and separable over F then we call K a *Galois* extension of F.

THEOREM 1.9. *(Existence and Uniqueness of the Splitting Field). If F is a field and f is any polynomial of positive degree in $F[x]$, then there exists a splitting field of f over F. Any two splitting fields of f over F are isomorphic under an isomorphism which fixes the elements of F (F-isomorphism) and sends roots of f into roots of f.*

PROOF. Let f be a polynomial of positive degree in $F[x]$. If g is a monic irreducible factor of f in $F[X]$, let $K = F[x]/(g)$. The mapping $a \mapsto a + (g)$ from F to K is a field homomorphism (sending 1_F to 1_K), therefore it is injective. We identify F with its image by identifying $a \in F$ with $a + (g)$. In this way we constructed a field K in which g, and therefore f, has a root. In fact, if $\alpha = x + (g) \in K$, then $g(\alpha) = g(x) + (g(x)) = 0 \in K$. If the degree of f is > 1, then the we can work with the polynomial $f_1 = f/(x - \alpha) \in K[x]$ and find an extension K_1 of K in which f_1 has a root, etc. Proceeding in this way we can find a field M in which

f splits in linear factors: $f(x) = a(x-\alpha_1)...(x-\alpha_n)$, with $\alpha_i \in M$, $a \in F$. Call $L = F(\alpha_1, ..., \alpha_n)$. Then L is a splitting field for f over F. This proves existence.

To prove uniqueness we proceed by induction on the degree d of f. If $d = 1$, then the splitting field for f over F is F. Suppose $d > 1$ and that the result is true for all polynomials of smaller degree. Let L_1 and L_2 be two splitting fields of f. Let g be a monic irreducible factor of f in $F[x]$, and $\alpha \in L_1, \beta \in L_2$ roots of g. By Theorem 1.7 (i) there is an F-isomorphism $F(\alpha) \to F(\beta)$, such that $\alpha \mapsto \beta$. Identify $F(\alpha)$ and $F(\beta)$ by means of this isomorphism and call this field F_1. Since $f/(x-\alpha) \in F_1[x]$ has degree $< d$, by induction hypothesis the splitting fields L_1 and L_2 of $f/(x-\alpha)$ are isomorphic, with an F_1-isomorphism ϕ sending roots of $f/(x-\alpha)$ into roots of $f/(x-\alpha)$. But then ϕ is also an F-isomorphism that sends roots of f into roots of f. (Note that this last property is automatic, since for any root α of f and any F-isomorphism $\phi : L_1 \to L_2$ we have $0 = \phi(0) = \phi(f(\alpha)) = f(\phi(\alpha))$.) $\square$

Since we are mainly interested in extension of finite fields, let us look some properties of finite fields.

PROPOSITION 1.10. *Let F be a finite field then*

(i) $CharF = p$ for some prime number and contains a field isomorphic to $F_p = \mathbb{Z}/p\mathbb{Z}$.

(ii) $|F| = p^n$, where $n = [F : F_p]$, the degree of F over F_p.

PROOF. (i) This has been proved at the begining of this chapter.

(ii) It is obvious, since for a given basis of F over F_p every element of F has a unique represention under this basis. $\square$

Let $F\times = F - \{0\}$ be the multiplicative group of finite field F then we have

THEOREM 1.11. *The multiplicative group $F^\times = F - \{0\}$ of a finite field is cyclic.*

PROOF. Let F be a finite field with p^n elements (p prime) and let $h = p^n - 1$. Factor h as $h = p_1^{r_1} \cdots p_m^{r_m}$ where p_i are distinct primes and $r_i \geq 1$. The group $F^\times$ has order h, so that we have to prove that there exists an element in $F^\times$ of order h. Let $h_i = h/p_i$. Since $h_i < h$ there exists an element $b_i \in F^\times$ which is not a root of $x^{h_i} - 1$. Let $a_i = b_i^{h/p_i^{r_i}}$ and $a = a_1 \cdots a_m$. We have $a_i^{p_i^{r_i}} = b_i^h = 1$ and so the order of a_i divides $p_i^{r_i}$. If $a_i^{p_i^{r_i-1}} = 1$ then $b_i^{h/p_i} = 1$, contrary to our choice of b_i. Hence the order of a_i is exactly $p_i^{r_i}$. Since $a^h = 1$ the order of a divides h. Suppose that this order is not h. Then there exists some prime divisor of h, say p_1, which divides h but does not divide the order of a as many as r_1 times. Then we have $a^{h/p_1} = a_1^{h/p_1} \cdots a_m^{h/p_1}$. Since $p_i^{r_i}$ divides h/p_1 for $i = 2, ..., m$, we have $a_1^{h/p_1} = 1$. This implies that $p_1^{r_i}$, the order of a_1, divides h/p_1, which is not true. Thus a has order h. $\square$

Note that if a is any generator of $F^\times$ then $F = F_p(a)$.

THEOREM 1.12. *(Existence and Uniqueness of Finite Fields) For any prime number p and any positive integer n there is one and (up to isomorphism) only one finite field with p^n elements. Any finite field with p^n elements is isomorphic to the splitting field of $x^{p^n} - x$ over F_p.*

PROOF. Let F denote the splitting field of the polynomial $x^{p^n} - x$ over F_p. Since the derivative of $x^{p^n} - x$ is $p^n x^{p^n - 1} - 1 = -1$ in $F_p[x]$, we have that $x^{p^n} - x$ has no

multiple roots. Let $S = \{a \in F : a^{p^n} - a = 0\}$, by Theorem 1.1 S is a subfield of F. On the other hand, Since S contains all roots of $x^{p^n} - x$, we have that $x^{p^n} - x$ must split in S. Thus $F = S$ and F is a finite field with p^n elements. This proves existence.

Now suppose that F is a finite field, by Proposition 1.10 $|F| = p^n$ for some prime p and some positive integer n, and F contains F_p as a subfield. Since $F^\times$ has order $p^n - 1$, we have $b^{p^n-1} = 1$ for all $b \in F^\times$. Therefore $b^{p^n} = b$ for all $b \in F$. So the p^n elements of F are precisely the roots of the polynomial $x^{p^n} - x$, and F is the splitting field of this polynomial ove F_p. Uniqueness now follows from Theorem 1.9.

From now on we call F_{p^n} the field with p^n elements. As consequences of Theorems 1.11 and 1.12 we have:

COROLLARY 1.13. *The finite field F_{p^n} is a simple extension of F_p. There exists an irreducible polynomial of degree n over F_p for every $n \geq 1$.*

THEOREM 1.14. *Let F_{p^n} be the finite field with p^n elements. Then every subfield of F_{p^n} has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there exists exactly one subfield of F_{p^n} with p^m elements.*

PROOF. Since any finite field has order p^m with p prime and m positive integer, the subfield of F_{p^n} must have order p^m with $m \leq n$. By Proposition 1.3, we have p^n must be the power of p^m, so that m is necessarily a divisor of n.

Conversely, if m is a divisor of n, then $p^m - 1$ divides $p^n - 1$ and so $x^{p^m-1} - 1$ divides $x^{p^n-1} - 1$ in $F_p[x]$. It follows that $x^{p^m} - x$ divides $x^{p^n} - x$ in $F_p[x]$. Thus all roots of $x^{p^m} - x$ are roots of $x^{p^n} - x$ so they belong to F_{p^n}, then F_{p^n} must contain

a splitting field of $x^{p^m} - x$ as its subfield and this splitting field has order p^m. The uniqueness is obvious, since the union of any two different subfields of order p^m of F_{p^n} would contain more than p^m roots of $x^{p^m} - x$. It is a contradiction. □

PROPOSITION 1.15. *Let F_q denote a finite field where q is a power of some prime number p. The polynomial $x^{q^n} - x$ is precisely the product of all the distinct irreducible polynomials in $F_q[x]$ of degree m, where m is a divisor of n.*

PROOF. Since $x^{q^n} - x$ has no multiple roots, it is a product of distinct irreducible polynomials in $F_q[x]$. Those irreducible factors of $x^{q^n} - x$ must have degrees dividing n. In fact, if α is a root of a an irreducible factor g of $x^{q^n} - x$ in $F_q[x]$, then degree$(g) = [F_q(\alpha) : F_q]$ is a divisor of n by Theorem 1.14. Now, let g be an irreducible polinomial in $F_q[x]$ of degree m, where $m|n$. If α is a root of g, then $F_q(\alpha) \simeq F_{q^m} \subseteq F_{q^n}$ by Theorem 1.14. Therefore $g|x^{q^n} - x$. □

Let F_q denote a finite field where q is a power of some prime number p, let F_{q^n} be a finite extension of F_q with degree n, then the field F_{q^n} is Galois over F_q (see [5], page 499), with cyclic Galois group $\mathcal{G} =< \sigma_q >$ of order n generated by Frobenius automorphism σ_q defined by $\sigma_q(a) = a^q$ for all $a \in F_q$. In other words we have

THEOREM 1.16. *The distinct automorphisms of F_{q^n} over F_q are exactly the mappings $1, \sigma_q, \sigma_q^2, ..., \sigma_q^{n-1}$, defined by $\sigma_q^i(a) = a^{q^i}$ for $a \in F_{q^n}$ and $0 \leq i \leq n-1$.*

THEOREM 1.17. *If f is an irreducible polynomial in $F_q[x]$ of degree n, then f has a root α in F_{q^n}. Furthermore, all the roots of f are simple and are given by the n distinct elements $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$ of F_{q^n}.*

PROOF. Let α be a root of f in the splitting field of f over F_q. Then $[F_q(\alpha) : F_q] = n$, hence $F_q(\alpha) = F_{q^n}$ and in particular $\alpha \in F_{q^n}$. The last part is clear by Theorem 1.16. $\square$

COROLLARY 1.18. *Let f be an irreducible polynomial in $F_q[x]$ of degree n. Then the splitting field of f over F_q is F_{q^n}.*

Chapter 2. Orthogonal Circulant Matrices over Finite fields.

Let F be the finite field with $q = p^m$ elements, where p is a prime. An $n \times n$ matrix A with entries in F is called circulant if A is of the form

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ . & . & . & . \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}.$$

We say that A is orthogonal if $A \cdot A^t = I$, where A^t is the transpose of A and I is the $n \times n$ identity matrix.

Let $O_{(n,q)}$ denote the set of $n \times n$ orthogonal circulant matrices of over F, then $O_{(n,q)}$ is a group under matrix multiplication. In this chapter we will discus how to find the cardinality of $O_{(n,q)}$. We will also give the tools to effectively construct this group when we know the factorization of $x^n - 1$ in $F[x]$, as is shown in the next chapters.

Let

$$T = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ . & . & . & . & . \\ 0 & . & . & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

For A circulant, as above, we can write $A = \sum_{i=0}^{n-1} a_i T^i$. Let $\mathcal{M}$ be the algebra of $n \times n$ circulant matrices over F. We start by giving a convenient representation for $\mathcal{M}$. Call $R_n = F[x]/(x^n - 1)$ the algebra of polynomials mod $(x^n - 1)$ over F. The following lemma shows that R_n is isomorphic to $\mathcal{M}$.

LEMMA 2.1. *The map $\varphi : \mathcal{M} \longrightarrow R_n$ defined by*

$$\varphi : \sum_{i=0}^{n-1} a_i T^i \longmapsto \sum_{i=0}^{n-1} a_i x^i$$

is an isomorphism of algebras.

PROOF. Let $\psi : F[x] \longrightarrow \mathcal{M}$ be the function defined by $\psi : f(x) \mapsto f(T)$. This function is clearly a surjective ring homomorphism and its kernel is the ideal generated by $(x^n - 1)$, since $x^n - 1$ is the minimum polynomial of T over F. So ψ induces an isomorphism $\overline{\psi} : R_n \to \mathcal{M}$. Now take $\varphi = \overline{(\psi)}^{-1}$. $\square$

Let $A = \sum_{i=0}^{n-1} a_i T^i$ and let $f(x) = \sum_{i=0}^{n-1} a_i x^i$ be the polynomial (modulo $x^n - 1$) corresponding to A by Lemma 2.1. The polynomial corresponding to A^t is $f(x)^t := \sum_{i=0}^{n-1} a_{n-i} x^i$ (indexes mod n). In fact, since $T^t = T^{-1}$, we have $A^t = \sum_{i=0}^{n-1} a_i T^{-i}$, and $f(x^{n-1}) = \sum_{i=0}^{n-1} a_i x^{(n-1)i} \equiv \sum_{i=0}^{n-1} a_i x^{-i} \equiv \sum_{i=0}^{n-1} a_{n-i} x^i = f(x)^t \bmod (x^n - 1)$ (where $a_n = a_0$). Therefore A is an orthogonal matrix if and only if $f(x) \cdot f(x)^t \equiv 1 \bmod (x^n - 1)$. The next proposition follows immediately from Lemma 2.1 and the definitions above.

PROPOSITION 2.2. *Let* $\mathcal{O} = \{f(x) \in R_n : f(x) \cdot f(x)^t = 1\}$. *Then* $\mathcal{O}$ *is a multiplicative group isomorphic to* $O_{(n,q)}$. *In particular* $|O_{(n,q)}| = |\mathcal{O}|$.

Call τ the automorphism of R_n given by $f \longmapsto f^t$ (it corresponds to transposition in $\mathcal{M}$). The following proposition is immediate.

PROPOSITION 2.3.

1) $\tau^2 =$ *identity.*

2) τ *fixes the elements of* F.

3) $\tau(x) = x^{-1} \pmod{(x^n - 1)}$.

We are interested in finding $O_{(n,q)}$. By Proposition 2.2, it is enough to find $\mathcal{O}$. We start by investigating properties of the ring R_n.

LEMMA 2.4. *If we factor the polynomial* $x^n - 1$ *as* $x^n - 1 = f_1^{n_1} \cdot f_2^{n_2} \cdots f_r^{n_r}$, *where* f_i $(1 \leq i \leq r)$ *are distinct monic irreducible polynomials of* $F[x]$, *then*

$$R_n \cong \frac{F[x]}{(f_1^{n_1})} \times \frac{F[x]}{(f_2^{n_2})} \times \cdots \times \frac{F[x]}{(f_r^{n_r})}.$$

(**Observation.** We will see later that actually $n_1 = \cdots = n_r = p^l$, where $p^l \| n$. For the moment this is not relevant to our discussion. In fact, the results of this part can be generalized by starting with an arbitrary orthogonal matrix T.)

PROOF. This is a special case of the Chinese Remainder Theorem. □

In what follows r, f_i and n_i are as in Lemma 2.4.

THEOREM 2.5. *Write, as above,* $x^n - 1 = \prod_{i=1}^{r} f_i^{n_i}$, *with* $f_i \in F[x]$ *distinct, irreducible, monic polynomials. Let* $R_n = F[x]/(x^n - 1)$, *then the following properties hold:*

1) R_n *is a principal ideal ring.*

2) There exist some elements $\{e_i : 1 \leq i \leq r\}$*(idempotents) in* R_n *such that*

i) $e_i \cdot e_j = \begin{cases} 0 & \text{if } i \neq j \\ e_i & \text{if } i = j. \end{cases}$

ii) $\sum_{i=1}^{r} e_i = 1.$

iii) For $1 \leq i \leq r$, *the ring* $e_i R_n$ *has a unique maximal ideal* $(\overline{f_i(x)})$ *and all its ideals have the form* $(\overline{f_i(x)})^j$, $0 \leq j \leq n_i$.

iv) $R_n = \bigoplus_{i=1}^{r} e_i R_n$, *and* $e_i R_n$ *is a ring isomorphic to* $F[x]/(f_i(x)^{n_i})$ *for* $1 \leq i \leq r$.

PROOF. 1) Every ideal $\mathcal{J}$ of R_n is of the form $\mathcal{J} \equiv \mathcal{I}/(x^n - 1)$, where $\mathcal{I}$ is an ideal of $F[x]$ containing $(x^n - 1)$. Since $F[x]$ is a principal ideal ring, $\mathcal{I}$ is principal. So $\mathcal{J}$ is also principal.

2) For $1 \leq i \leq r$, let $p_i(x) = f_1^{n_1} \cdot f_2^{n_2} \cdots f_{i-1}^{n_{i-1}} \cdot f_{i+1}^{n_{i+1}} \cdots f_r^{n_r} = \frac{x^n - 1}{f_i(x)^{n_i}}$. Since $p_i(x)$ and $f_i(x)^{n_i}$ are relatively prime, there exists $q_i(x) \in F[x]$ such that $p_i(x) \cdot q_i(x) \equiv 1 \mod f_i(x)^{n_i}$. We let $E_i = p_i(x) \cdot q_i(x) \in F[x]$ and let e_i be the class of E_i mod $(x^n - 1)$. We have $E_i^2 \equiv 1^2 \equiv E_i \mod f_i(x)^{n_i}$ and $E_i^2 \equiv 0^2 \equiv E_i \mod f_j(x)^{n_j}$ for $i \neq j$. Therefore $E_i^2 \equiv E_i$ and $E_i \cdot E_j \equiv 0 \mod (x^n - 1)$ for $i \neq j$. Correspondingly we have $e_i^2 = e_i$ and $e_i \cdot e_j = 0$ for $i \neq j$. By the construction of the E_i, we have $\sum_{j=1}^{r} E_j \equiv 1 \mod f_i(x)^{n_i}$ for $1 \leq i \leq r$, so that $\sum_{j=1}^{r} E_j \equiv 1 \mod (x^n - 1)$, Thus $\sum_{i=1}^{r} e_i = 1$.

By ii) we have $\bigoplus_{i=1}^{r} e_i R_n = R_n$ which, by i), is a direct sum. Let $\phi : F[x] \longrightarrow e_i R_n$ be the ring homomorphism defined by $f \longmapsto \overline{f}$, where $\overline{f} = e_i(f + (x^n - 1)) \in e_i R_n$. It is clear that ϕ is surjective and the kernel of ϕ is the ideal of $F[x]$ generated by $f_i(x)^{n_i}$. So $e_i R_n \cong F[x]/(f_i(x)^{n_i})$. We know that $F[x]/(f_i(x)^{n_i})$, as R_n, is a principal ideal ring. By [9], Theorem 2.6, we have a one to one order-preserving correspondence between the ideals of $F[x]/(f_i(x)^{n_i})$ and the ideals of $F[x]$ containing $f_i(x)^{n_i}$. Thus all ideals of $F[x]/(f_i(x)^{n_i})$ are powers of $(\overline{f_i(x)})$ and since $f_i(x)$ is irreducible in $F[x]$ we have that $(\overline{f_i(x)})$ is the unique maximal ideal of $F[x]/(f_i(x)^{n_i})$. So the ring $e_i R_n$ is a local ring. □

Theorem 2.5 shows that the maximal ideal of $e_i R_n$ is $M = (\overline{f_i(x)})$ and that all

its ideals are powers of M. Also, M is nilpotent since $(\overline{f_i(x)})^{n_i} = (0)$. Therefore the lattice of ideals of e_iR_n is of the form $e_iR_n \supset M \supset M^2 \supset M^3 \supset \cdots \supset M^{n_i} = (0)$.

Since for each e_i associate with exactly one irreducible factor g_i of $x^n - 1$ ($e_iR_n \cong F[x]/(f_i(x)^{n_i})$ and the automorphism τ of R_n will send g_i to g_i^t by the definition but g_i^t is an irreducible factor of $x^n - 1$ ($\tau(x^n - 1) = 1 - x^n$ and g_i is an irreducible factor of $x^n - 1$), the automorphism τ of R_n must permute the members of the set $\xi = \{e_i : 1 \leq i \leq r\}$. Since τ^2 =identity, the orbits of τ in ξ are either of the form $\{e_i\}$ with $\tau(e_i) = e_i$ or of the form $\{e_i, e_j\}$ with $i \neq j$ and $\tau(e_i) = e_j$. In the first case we call the orbit a 1-cycle and in the second case we call the orbit a 2 cycle.

Let $\xi_1, ..., \xi_t$ be the distinct orbits of τ in ξ. Then the ξ_k are pairwise disjoint and $\xi = \cup_{k=1}^t \xi_k$.

For $1 \leq k \leq t$, let $\Im_k = \oplus_{e \in \xi_k} eR_n$ be the ideal generated by a given orbit ξ_k. Then $\Im_k$ is a direct sum of the rings eR_n, $e \in \xi_k$. Whether the given orbit is a 1-cycle or a 2-cycle, the transpose map τ of R_n acts on each $\Im_k$ as an automorphism by restriction. Since $\bigoplus_{i=1}^r e_iR_n = R_n$ we have $R_n = \sum_{k=1}^t \Im_k$ (direct sum). Correspondingly we have the group decomposition $\mathcal{O} \cong \prod_{k \in K}^t \mathcal{O}\,|_{\Im_k}$, thus to find $\mathcal{O}$ it is enough to study the orthogonal group in each orbit. Since an orbit is either a 1-cycle or a 2-cycle, we will work on two types of rings: (1) the local ring e_iR_n where $\tau(e_i) = e_i$ and (2) the ring $e_iR_n \times e_jR_n$ where e_iR_n and e_jR_n are isomorphisc local rings and $\tau\,|_{e_iR_n \times 0}$ and $\tau\,|_{0 \times e_jR_n}$ are inverse isomorphisms.

In what follows $\mathbb{F}$ is an arbitrary field (we are mostly interested in the case $\mathbb{F} = F$).

DEFINITION. *Let $\psi(x) \in \mathbb{F}[x]$, and let $R = \mathbb{F}[x]/(\psi(x))$. If an automorphism τ of R satisfies the conditions*

(1) $\tau^2 =$ identity,

(2) τ fixes the elements of $\mathbb{F}$,

(3) $\tau(x) = x^{-1} \pmod{\psi(x)}$

(see Proposition 2.3), then we call τ the transpose map of R.

DEFINITION. *A polynomial $f(x)$ of $F[x]$ is said to be reciprocal if $f(0) \neq 0$ and whenever α is a root of $f(x)$ of multiplicity m, then α^{-1} is also a root of $f(x)$ of multiplicity m.*

The following proposition gives a characterization of the reciprocal polynomials not divisible by $x - 1$.

PROPOSITION 2.6. *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$. Suppose $f(0) \neq 0$ and $f(1) \neq 0$. Then $f(x)$ is reciprocal if and only if $a_i = a_{n-i}$ for each i, $0 \leq i \leq n$.*

PROOF. Suppose $f(x)$ is reciprocal, and let α be a root of $f(x)$. It may happen that $\alpha = \alpha^{-1}$, then we have $\alpha^2 = 1$, in this case (since $f(1) \neq 0$) we have $\alpha = -1$. Therefore by the definition above, we can factor $f(x)$ as $f(x) = (x+1)^l \prod_{k=1}^{r}(x - \alpha_k)(x - \alpha_k^{-1})$ for some l and r, where $\alpha_k \neq \alpha_k^{-1}$. Since $(x - \alpha_k)(x - \alpha_k^{-1}) = x^2 - (\alpha_k + \alpha_k^{-1})x + 1$ and $(x+1)$ both satisfy $a_i = a_{n-i}$, and since products of such polynomials are still the polynomials which satisfy $a_i = a_{n-i}$ for their coefficients, $f(x)$ satisfies the condition $a_i = a_{n-i}$.

Conversely, suppose $f(x)$ satisfies $a_i = a_{n-i}$. Let α be any root of $f(x)$. We have $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + \cdots + a_1 \cdot \alpha + a_0 = 0$. Multiplying this equality by α^{-n} , we

obtain $a_n + a_{n-1} \cdot \alpha^{-1} + \cdots + a_1 \cdot \alpha^{-(n-1)} + a_0 \cdot \alpha^{-n} = 0$ so that $f(\alpha^{-1}) = 0$ because $f(x)$ satisfies $a_i = a_{n-i}$. We have to prove that whenever α is a root of $f(x)$ of multiplicity m, then α^{-1} is also a root of $f(x)$ of multiplicity m. If $\alpha = \alpha^{-1}$, that is clear. Suppose $\alpha \neq \alpha^{-1}$; we prove by induction on k that if $(x-\alpha)^k \| f(x)$ then $(x-\alpha^{-1})^k \| f(x)$. For $k = 1$ the result follows from the comment at the beginning of this paragraph. Now suppose that our affirmation is true for the integer k and that $(x-\alpha)^{k+1} \| f(x)$. Then we can write $f(x) = (x+1)^l (x-\alpha)^k (x-\alpha^{-1})^k \cdot h(x)$ where $(h(x), x+1) = 1$. Since $f(x)$ and $(x+1)^l (x-\alpha)^k (x-\alpha^{-1})^k$ are symmetric, we have that $h(x)$ is symmetric. Also $h(\alpha) = 0$. Therefore $h(\alpha^{-1}) = 0$. That implies that $x - \alpha^{-1} \| h(x)$ and so $(x-\alpha^{-1})^{k+1} \| f(x)$. Clearly this implies that the multiplicities of α and α^{-1} as roots of $f(x)$ are equal. $\square$

Let $R = \mathbb{F}[x]/(\psi(x))$ where $\psi(x) = g_1(x)^{n_1} \cdot g_2(x)^{n_2} \cdots g_r(x)^{n_r}$, and the $g_i(x)$ $(1 \leq i \leq r)$ are irreducible and distinct in $\mathbb{F}[x]$. Suppose there is a transpose map τ in R. Arguing as in Theorem 2.5, we can show that $R \cong e_1 R \times e_2 R \times \cdots \times e_r R$ where each $e_i R$, for $1 \leq i \leq r$ is the local ring associated with the factor $g_i^{n_i}$. The map τ permutes the set $\{e_1, e_2, \cdots, e_r\}$ and induces a decomposition of this set in 1-cycles and 2-cycles. At 1-cycle $\{e_i\}$ (so $\tau(e_i) = e_i$) the effect of τ is to produce an automorphism of $\mathbb{F}[x]/(g_i^{n_i})$. At 2-cycle $\{e_i, e_j\}$ (so $i \neq j$ and $\tau(e_i) = e_j$) the effect of τ is to produce an isomorphism from $\mathbb{F}[x]/(g_i^{n_i})$ to $\mathbb{F}[x]/(g_j^{n_j})$. In this case the maximal ideals of $\mathbb{F}[x]/(g_i^{n_i})$ and $\mathbb{F}[x]/(g_j^{n_j})$ are generated by the cosets of g_i and g_j respectively, and since τ must match powers of the respective maximal ideals of $\mathbb{F}[x]/(g_i^{n_i})$ and $\mathbb{F}[x]/(g_j^{n_j})$, we have $n_i = n_j$. We also have that $\deg(g_i) = \deg(g_j)$ because the transpose map $\mathbb{F}[x]/(g_i) \longrightarrow \mathbb{F}[x]/(g_j)$ induced by τ is an isomorphism.

We want to show that if $\psi(x) \in \mathbb{F}[x]$ then $\mathbb{F}[x]/(\psi(x))$ has a transpose map if and only if ψ is a reciprocal polynomial. We prove first

PROPOSITION 2.7. *If $R = F[x]/(\psi(x))$ has a transpose map, then $\psi(x)$ is reciprocal.*

PROOF. We write $\psi(x) = \prod_{i=1}^{r} g_i^{n_i}$ with the idempotents $\{e_1, e_2, \cdots, e_r\}$ as above, let $1 \leq i \leq r$ and suppose $\tau(e_i) = e_j$ with $i \neq j$, namely $\{e_i, e_j\}$ is a 2-cycle. Then τ induces an isomorphism from $\mathbb{F}[x]/(g_i^{n_i})$ to $\mathbb{F}[x]/(g_j^{n_i})$ where $\deg(g_i) = \deg(g_j)$. Let τ' be the isomorphism induced by τ from $\mathbb{F}[x]/(g_i)$ to $\mathbb{F}[x]/(g_j)$. Since τ sends x to x^{-1} and fixes the elements of $\mathbb{F}$, for $x + (g_i) \in \mathbb{F}[x]/(g_i)$,

$$(*) \qquad \tau'(x + (g_i)) = (x + (g_j))^{-1}.$$

Let $g_i(\alpha_i) = 0$ and $g_j(\alpha_j) = 0$. Since $\mathbb{F}(\alpha_i) \cong \mathbb{F}[x]/(g_i)$ (with $\alpha_i \mapsto \overline{x}$) and $\mathbb{F}(\alpha_j) \cong \mathbb{F}[x]/(g_j)$ (with $\alpha_j \mapsto \overline{x}$), by $(*)$ there exists an isomorphism from $\mathbb{F}(\alpha_i)$ to $\mathbb{F}(\alpha_j)$ that sends α_i to α_j^{-1}. So $g_i(\alpha_j^{-1}) = 0$. It follows easily that the roots of $g_i(x)$ are the inverse roots of $g_j(x)$. Since these polynomials have the same degree and since all roots of an irreducible polynomial have the same multiplicity, we have that the multiplicity of α_i as a root of g_i is the same as the multiplicity of α_i^{-1} as a root of g_j. So $(g_i(x)g_j(x))^{n_i}$ is reciprocal.

If $\tau(e_i) = e_i$ for $1 \leq i \leq r$, clearly any root α_i of g_i has the same multiplicity as the root α_i^{-1}. This shows that we can write $\psi(x)$ as a product of reciprocal polynomials. Therefore $\psi(x)$ is reciprocal. $\square$

Now let us consider the converse of Proposition 2.7. Suppose that $\psi(x)$ is reciprocal, and we factor it as $\psi(x) = g_1(x)^{n_1} \cdot g_2(x)^{n_2} \cdots g_r(x)^{n_r}$ where g_i are irreducible and distinct in $\mathbb{F}[x]$. Let $g_i(x) = \prod_{l=1}^{k}(x-\alpha_l)$ be an irreducible factor of $\psi(x)$. Then $g_j(x) = \prod_{l=1}^{k}(x-\alpha_l^{-1})$ is also an irreducible factor since $\psi(x)$ is reciprocal, and it is clear $g(x)_j \| \psi(x)$ and for each α_l, α_l^{-1} has the same degree as α_l over $\mathbb{F}$. Suppose $g_i \neq g_j$, (if $g_i = g_j$ we have a similar and simpler situation). Then we have that g_i and g_j have the same degree, the same multiplicity $k = n_i = n_j$ (since $\psi(x)$ is reciprocal), and the same splitting field over $\mathbb{F}$. We will construct an isomorphism $\tau : \mathbb{F}[x]/(g_i^k) \longrightarrow \mathbb{F}[x]/(g_j^k)$ which fixes the elements of $\mathbb{F}$ and sends $x + (g_i^k)$ to $(x + (g_j^k))^{-1}$. Then τ will be a transpose map corresponding to the 2-cycle $\{e_i, e_j\}$. Since R is a direct sum of the ideals $\Im_j = \oplus_{e \in \xi_j} eR$ which are generated by distinct orbits (2-cycles and 1-cycles), this construction will give a transpose map on R.

We define ϕ_{g_i} the natural projection from $\mathbb{F}[x]$ to $\mathbb{F}[x]/(g_i^k)$ that is

$$\phi_{g_i} : \quad a \mapsto a \quad \text{if} \quad a \in \mathbb{F}$$

$$x \mapsto \overline{x} = x + (g_i^k).$$

LEMMA 2.8. *$\mathbb{F}[x]/(g_j^k)/(\phi_{g_j}(g_j))$ is isomorphic to $\mathbb{F}[x]/(g_j)$.*

PROOF. Let λ be the usual ring homomorphism from $\mathbb{F}[x]$ to $\mathbb{F}[x]/(g_j^k)/(\phi_{g_j}(g_j))$, then for $h \in \mathbb{F}[x], \lambda(h) = \overline{h} = (h + (g_j^k)) + (\phi_{g_j}(g_j)) = (h + (g_j^k)) + (g_j + (g_j^k))$. So h is in the kernel of λ if and only if $g_j \| h$. Also λ is surjective. Thus $\mathbb{F}[x]/(g_j) = \mathbb{F}[x]/\ker(\lambda) \cong (\mathbb{F}[x]/(g_j^k))/(\phi_{g_j}(g_j))$. $\square$

PROPOSITION 2.9. *If $\psi(x)$ is reciprocal then $R = \mathbb{F}[x]/(\psi(x))$ has a transpose map.*

PROOF. As we explained above it is enough to construct the isomorphism $\tau : \mathbb{F}[x]/(g_i^k) \longrightarrow \mathbb{F}[x]/(g_j^k)$ where g_i, g_j are irreducible polynomials whose roots are mutually reciprocal and $g_i^k, g_j^k \| \psi(x)$. Assume $g_j \neq g_i$, let ϕ_{g_i} and ϕ_{g_j} be the ring maps defined above. Since g_i and g_j are irreducible polynomials in $\mathbb{F}[x]$, we have that $\phi_{g_i}(x)$ and $\phi_{g_j}(x)$ are both invertible elements. Let φ be the homomorphism from $\mathbb{F}[x]$ to $\mathbb{F}[x]/(g_j^k)$ defined by

$$\varphi : \qquad a \mapsto a \qquad \text{if} \quad a \in \mathbb{F}$$

$$x \mapsto \phi_{g_j}(x)^{-1}$$

Let us consider the map sequence

$$\mathbb{F}[x] \overset{\varphi}{\longrightarrow} \mathbb{F}[x]/(g_j^k) \overset{\pi}{\longrightarrow} \mathbb{F}[x]/(g_j^k)/(\phi_{g_j}(g_j)) \cong \mathbb{F}[x]/(g_j)$$

where π is the natural projection. Then $\pi \cdot \varphi(x) = (x + (g_j))^{-1}$. Call $\omega = \pi \cdot \varphi$. We have that $\omega(x) = (x + (g_j))^{-1}$ and that $\omega(a) = a$ for all $a \in \mathbb{F}$. Then we have $\omega(g_i(x)) = g_i(\omega(x)) = g_i((x + (g_j))^{-1})$. Since $x + (g_j)$ is a root of g_j and since g_i and g_j have mutually inverse roots, we have $g_i((x + (g_j))^{-1}) = 0$. It follows that $\pi \cdot \varphi(g_i) = 0$. So that $\varphi(g_i) \in (\phi_{g_j}(g_j))$. Then $\varphi(g_i^k) = [\varphi(g_i)]^k = 0$. Thus the kernel of φ contains the ideal generated by (g_i^k). Then φ induces an homomorphism τ from $\mathbb{F}[x]/(g_i^k)$ to $\mathbb{F}[x]/(g_j^k)$ and sends $x + (g_i^k)$ to $(x + (g_j^k))^{-1}$. It follows that τ is an isomorphism (recall that g_i and g_j have the same degree). Similarly, there exists

an isomorphism τ' from $\mathbb{F}[x]/(g_j^k)$ to $\mathbb{F}[x]/(g_i^k)$ and sending $x+(g_j^k)$ to $(x+(g_i^k))^{-1}$. If we assume $g_i = g_j$, we obtain in a similar way an automorphism τ of $\mathbb{F}[x]/(g_i^k)$ sending $x+(g_i^k)$ to $(x+(g_i^k))^{-1}$. $\square$

Combining Propositions 2.7 and 2.9, we obtain

THEOREM 2.10. *If $\mathbb{F}$ is a field and $\psi(x) \in \mathbb{F}[x]$ then $\psi(x)$ is reciprocal if and only if $\mathbb{F}[x]/(\psi(x))$ has a transpose map.*

Let $\psi(x) = g_1(x)^{n_1} \cdot g_2(x)^{n_2} \cdots g_r(x)^{n_r}$ and let τ be a transpose map of $\mathbb{F}[x]/(\psi(x))$ where the $g_i(x)$ are irreducible in $\mathbb{F}[x]$. By Theorem 2.10, if g_i corresponds to a 1-cycle then g_i is reciprocal, and if g_i, g_j correspond to a 2-cycle then they are nonreciprocal, have the same degree and $g_i \cdot g_j$ is reciprocal. If g_i is an irreducible reciprocal polynomial and $(g_i, x \pm 1) = 1$ then g_i has even degree because the roots α and α^{-1} of g_i are distinct and have the same multiplicity.

Recall that our main purpose is to study $\mathcal{O}$, and to find a formula for $|\mathcal{O}|$. We will begin our discussion with the 1-cycle case.

1-CYCLE CASE.

Suppose that $g(x)$ is an irreducible reciprocal factor of $\psi(x)$ with multiplicity m. Let $R = F[x]/(\psi(x))$ and $R' = F[x]/(g^m)$. Let e be the idempotent corresponding to R', i.e. $eR \cong R'$, and let M be the maximal ideal of R', which is generated by the coset of $g(x)$. Note that M is nilpotent: $M^m = 0$.

Let $\tau : R' \longrightarrow R'$ be a transpose map. The simplest case occurs when $m = 1$ and $g = x \pm 1$.

PROPOSITION 2.11. *With g and τ as above, $g = x \pm 1$ and $m = 1$ if and only if τ is the identity.*

PROOF. If $g(x) = x \pm 1$, then $\overline{x} = x + (g) = \mp\overline{1}$ so $\tau(\overline{x}) = \overline{x}^{-1} = \overline{x}$, it follows that τ is the identity. Conversely if τ is the identity, since $\overline{x} \cdot \tau(\overline{x}) = \overline{x}^2 = \overline{1}$ we must have $\overline{x} = \pm\overline{1}$ and so that $g(x) = x \pm 1$ and $m = 1$. $\square$

Let us return to the general situation (g irreducible reciprocal). The following lemma gives a simple description of the quotient rings of R'.

LEMMA 2.12. *$R'/M^i \cong F[x]/(g(x)^i)$ for $1 \leq i \leq m$.*

PROOF. For $1 \leq i \leq m$, let

$$\rho : F[x] \longrightarrow R'/(\overline{g(x)^i})$$

$$f(x) \mapsto \overline{f(x)} + (\overline{g(x)^i})$$

be the composition of the natural projections $F[x] \longrightarrow R', f(x) \mapsto \overline{f(x)} = f(x) + (g(x)^m)$ and $R' \longrightarrow R'/(\overline{g(x)^i}), \overline{f(x)} \mapsto \overline{f(x)} + (\overline{g(x)^i})$. Let $f(x) \in \ker\rho$, then $\overline{f(x)} \in (\overline{g(x)^i})$. We have $\overline{f(x)} = \overline{g(x)^i} \cdot \overline{h(x)}$ for some $h(x) \in F[x]$. Thus $f(x) = g(x)^i \cdot h(x) + (g(x)^m)$. So $g(x)^i \| f(x)$. It follows that $f(x) \in (g(x)^i)$. This shows that $\ker\rho \subseteq (g(x)^i)$. It is obvious that $(g(x)^i) \subseteq \ker\rho$. Therefore $\ker\rho = (g(x)^i)$ and the lemma follows. $\square$

Let τ be the transpose map of R'. For $1 \leq i \leq m$ we define τ_i as the automorphism of $R'/M^i \cong F[x]/(g(x)^i)$ such that

$$\tau_i(r + (g(x)^i)) = \tau(r) + (g(x)^i) \quad \text{where} \quad r \in R'.$$

Clearly τ_i is a transpose map on R'/M^i:

$$R'/M^i \xrightarrow{\tau_i} R'/M^i.$$

In particular

$$R' = R'/M^m \xrightarrow{\tau=\tau_m} R'/M^m \qquad (M^m = 0).$$

Recall that $\mathcal{O} = \{f(x) \in R : f(x) \cdot f(x)^t = 1\}$. Call $\mathcal{O}' = \{f(x) \in R' : f(x) \cdot f(x)^t = 1\}$ and $\mathcal{O}_i = \{f(x) \in R'/M^i : f(x) \cdot \tau_i(f(x)) = 1\}$.

For $i \geq 2$, let

$$\varphi_i : R'/M^i \longrightarrow R'/M^{i-1}$$

be the application

$$r + M^i \mapsto r + M^{i-1}$$

φ_i is a ring epimorphism. We have $\varphi_i(\mathcal{O}_i) \subseteq \mathcal{O}_{i-1}$, so φ_i is a group homomorphism from $\mathcal{O}_i$ to $\mathcal{O}_{i-1}$. If all maps φ_i are surjective then by composing them, we construct a surjective map $\varphi' : \mathcal{O} \longrightarrow \mathcal{O}_1$, and $\mathcal{O}/\ker\varphi' \cong \mathcal{O}_1$. Since $\mathcal{O}_1 \subseteq R'/M$ and R'/M is a field, $|\mathcal{O}_1|$ is relatively easy to find, thus in order to find $|\mathcal{O}|$ it is enough to determine $|\ker\varphi'|$.

THEOREM 2.13. *Let F be a field and let $F[x]$ the polynomial ring in one variable. Let f, $h \in F[x]$, and assume deg $h \geq 1$. Then there exist unique polynomials*

$$f_0, f_1 \cdots f_n \in F[x]$$

such that either $f_i = 0$ *or deg* $f_i <$ *deg* h *and*

$$f = f_0 + f_1 h + \cdots + f_n h^n$$

(see [2], Page 196).

The expression of f in Theorem 2.13 is called the h-adic representation of f. By this theorem, taking $h = g$, for every $f \in R'$ we have that $f = f_0 + f_1 g + \cdots + f_{m-1} g^{m-1}$ ($f_i = 0$ or deg $f_i <$ deg g), where we can regard the f_i as belonging to the field R'/M.

We will think of R'/M^i as the set of polynomials in $F[x]$ of degree less than the degree of $g^i(x)$ with the usual addition and multiplication mod $g^i(x)$. In this way we have all the R'/M^i as subsets of R'. We will always suppose that the elements of R'/M^i are represented g-adically. Our purpose is to determine when the polynomial f belongs to $\mathcal{O}'$.

Let $f = \sum_{j=0}^{m-1} f_j g^j \in \mathcal{O}'$ (g-adic representation). Then for $0 \leq l \leq m$ we regard $\sum_{j=0}^{l-1} f_j g^j$ as an element of $\mathcal{O}_l$ where $\sum_{j=0}^{l-1} f_j g^j$ is a simple truncation of the g-adic representation. In this way we have $f_0 \in \mathcal{O}_1$, $f_0 + f_1 g \in \mathcal{O}_2$, etc. So, to construct an element of $\mathcal{O}'$ we can select first an element $f_0 \in \mathcal{O}_1$, and then we must find an element $f_1 \in R'/M$ such that $f_0 + f_1 g \in \mathcal{O}_2$, ..., an element $f_{m-1} \in R'/M$ such that $f_0 + f_1 g + \cdots + f_{m-1} g^{m-1} \in \mathcal{O}_m = \mathcal{O}'$. Let $1 \leq i \leq m$. If $f \in R'$ let $\sum_{j=0}^{m-1} d_j g^j$ be the g-adic representation of $f \cdot \tau(f) - 1$. We call d_j the jth **deviation** of g.

LEMMA 2.14. *Let* $1 \leq i \leq m-1$. *If* $f' = \sum_{j=0}^{i-1} f_j g^j \in R'/M^i$ *and* $f' \in \mathcal{O}_i$ *then there exists* f_i *such that* $f = f' + f_i g^i \in \mathcal{O}_{i+1}$ *if and only if* $d_i = 0$ *where* d_i *is the* i*th deviation of* f.

PROOF. Suppose that $f = f' + f_i g^i \in \mathcal{O}_{i+1}$ then $f \cdot \tau_{i+1}(f) - 1 \equiv 0 \bmod g^{i+1}$. That is $\sum_{j=0}^{i} d_j g^j \equiv 0 \bmod g^{i+1}$. So we have $d_0 = d_1 = \cdots = d_i = 0$. Conversely, suppose $d_i = 0$. Since also $f \in \mathcal{O}_i$ we have $d_0 = d_1 = \cdots = d_{i-1} = d_i = 0$ so $f \cdot \tau(f) - 1 = d_{i+1} g^{i+1} + d_{i+2} g^{i+2} + \cdots$. That is $f \cdot \tau_{i+1}(f) - 1 \equiv f \cdot \tau(f) - 1 \equiv 0 \bmod g^{i+1}$. Therefore $f = f' + f_i g^i \in \mathcal{O}_{i+1}$. □

Recall that τ is a transpose map of R'; in particular it is an automorphism of R'. Since $M = (g)$ is the only maximal ideal of R', we must have $M = \tau(M) = (\tau(g))$. So $\tau(g) = u \cdot g$ for some unit u of R'. Let $\beta : R' \longrightarrow R'/M$ be the canonical projection. Call $\beta(u) = u_0$.

LEMMA 2.15. *Let* u *be the unit of* R' *such that* $\tau(g) = u \cdot g$ *and let* u_0 *be the canonical image of* u *in* R'/M. *If* $m \geq 2$ *then* $u_0 \in \mathcal{O}_1$.

PROOF. Recall that $R' = F[x]/(g^m)$. Suppose $m \geq 2$. Since $\tau(g) = u \cdot g$, we have $\tau^2(g) = \tau(u \cdot g) = \tau(u)\tau(g)$, but $\tau^2 = 1$, so that $g = \tau(u) \cdot u \cdot g$, thus $(\tau(u) \cdot u - 1) \cdot g = 0$ in R'. Since $g \neq 0$ then $\tau(u) \cdot u - 1$ is not an unit, but R' is a local ring i.e. it has a unique maximal ideal M, so $\tau(u) \cdot u - 1 \in M$. Thus $\tau(u) \cdot u \equiv 1 \bmod g$, which means $u_0 \cdot \tau_1(u_0) = 1$ in R'/M. □

THEOREM 2.16. *Let* $1 \leq i \leq m-1$ *and let* $f = \sum_{j=0}^{i-1} f_j g^j \in \mathcal{O}_i$, *then* $f + f_i g^i \in \mathcal{O}_{i+1}$ *if and only if* f_i *satisfies (in* R'/M*)*

$$\tau_1(f_i \cdot f_0^{-1})u_0^i + (f_i \cdot f_0^{-1}) = -d_i$$

where d_i is the ith deviation of f.

PROOF. Suppose $f + f_i g^i \in \mathcal{O}_{i+1}$ then $(f + f_i g^i) \cdot \tau_{i+1}(f + f_i g^i) \equiv (f + f_i g^i) \cdot \tau(f + f_i g^i) \equiv 1 \bmod g^{i+1}$ so we have $f \cdot \tau(f) + f \cdot \tau(f_i g^i) + f_i g^i \cdot \tau(f) \equiv 1 \bmod g^{i+1}$. i.e. $f \cdot \tau(f) - 1 + f \cdot \tau(f_i) \cdot u^i \cdot g^i + f_i g^i \cdot \tau(f) \equiv 0 \bmod g^{i+1}$. Since $f \in \mathcal{O}_i$ it follows from the definition of the deviation d_i that $f \cdot \tau(f) - 1 \equiv d_i g^i \bmod g^{i+1}$(since $d_j = 0$, $0 \leq j \leq i-1$) . So $d_i g^i + f \cdot \tau(f_i) \cdot u^i \cdot g^i + f_i g^i \cdot \tau(f) \equiv 0 \bmod g^{i+1}$. Thus $(d_i + f_i \cdot \tau(f) + f \cdot \tau(f_i) \cdot u^i) \cdot g^i \equiv 0 \bmod g^{i+1}$, which means $d_i + f_i \cdot \tau(f) + f \cdot \tau(f_i) \cdot u^i \equiv 0 \bmod g$. That is $d_i + f_i \cdot \tau_1(f_0) + f_0 \cdot \tau(f_i) \cdot u^i \equiv 0 \bmod g$. Since $f_0 \in \mathcal{O}_1$, $\tau_1^2 = 1$, and u_0 is the image of u in R'/M, $\tau(f_0) \equiv f_0^{-1} \bmod g$ and we have $d_i + f_i \cdot f_0^{-1} + \tau_1(f_0^{-1} \cdot f_i) \cdot u_0^i \equiv 0 \bmod g$. Since the process above is invertible, the converse is obvious. □

Recall that τ_1 is the transpose map of R'/M, so either τ_1 has period two or τ_1 is the identity. Let F_1 be the fixed field of τ_1 in R'/M, then $\tau_1 + 1$ is an F_1-linear endomorphism of R'/M.

THEOREM 2.17.

1) If $\tau_1 \neq 1$ or Char $F \neq 2$, then $ker(\tau_1 + 1) = \{r \in R'/M : \tau_1(r) = -r\}$ and $Im(\tau_1 + 1) = F_1$.

2) $ker(\tau_1 + 1) = rF_1$ for some $r \in R'/M$.

3) Let $r \in (R'/M)^\times$, then $r^{-1}\tau_1(r) \in \mathcal{O}_1$ and the map $r \mapsto r^{-1}\tau_1(r)$ from $(R'/M)^\times$ to $\mathcal{O}_1$ is onto unless $\tau_1 = 1$ and Char $F \neq 2$.

PROOF. 1) If $r \in R'/M$ and $\tau_1(r) = -r$ then $(\tau_1 + 1)(r) = 0$. Conversely, if $r \in ker(\tau_1 + 1)$ then $(\tau_1 + 1)(r) = \tau_1(r) + 1(r) = \tau_1(r) + r = 0$, so that $\tau_1(r) = -r$. Let $r \in Im(\tau_1 + 1)$ then there exists $r' \in R'/M$ such that $(\tau_1 + 1)(r') = r$ then $\tau_1(r) = \tau_1 \cdot (\tau_1 + 1)(r') = (\tau_1 + 1)(r') = r$, thus $r \in F_1$. This proves that $\mathrm{Im}(\tau_1 + 1) \subseteq F_1$. Conversely, if Char $F \neq 2$, then for every $f \in F_1$ we have $(\tau_1 + 1)(f) = 2f$. Since $2 \neq 0$ we have $f = (\tau_1 + 1)(\frac{1}{2}f)$. Thus $F_1 \subseteq Im(\tau_1 + 1)$. If Char $F = 2$ and $\tau_1 \neq 1$, let $x_0 \in R'/M$ be an element such that $\tau_1(x_0) \neq x_0$, then $(\tau_1 + 1)(x_0) \neq 0$. Call $y_0 = (\tau_1 + 1)(x_0)$, we have $(\tau_1 + 1)(\frac{x_0}{y_0}) = 1$. So there exists an element $x \in R'/M$ such that $(\tau_1 + 1)(x) = 1$. It follows that for every $f \in F_1$ we have $(\tau_1 + 1)(xf) = xf + \tau_1(xf) = xf + \tau_1(x)f = (x + \tau_1(x))f = f$. Therefore $F_1 \subseteq Im(\tau_1 + 1)$. So, in both cases, $Im(\tau_1 + 1) = F_1$.

2) If $ker(\tau_1 + 1) = \{0\}$ then we take $r = 0$. Suppose $ker(\tau_1 + 1) \neq \{0\}$. Let $r' \neq 0$ such that $r' \in ker(\tau_1 + 1)$ then $\tau_1(r') = -r'$. Since for every $r \in ker(\tau_1 + 1)$, $\tau_1(r) = -r$ we have $\tau_1(\frac{r}{r'}) = \frac{r}{r'}$. So $\frac{r}{r'} \in F_1$, i.e. $r \in r'F_1$. Conversely, for any $r'r \in r'F_1$, we have $\tau_1(r'r) = -r'r$. i.e. $r'r \in ker(\tau_1 + 1)$. Therefore $ker(\tau_1 + 1) = r'F$.

3) Since $(r^{-1}\tau_1(r))\tau_1(r^{-1}\tau_1(r)) = r^{-1}\tau_1(r) \cdot (\tau_1(r))^{-1}r = 1$ we have $r^{-1}\tau_1(r) \in \mathcal{O}_1$. To prove that the map $(R'/M)^\times \longrightarrow \mathcal{O}_1$, $r \mapsto r^{-1}\tau_1(r)$ is surjective we use the idea of the proof of Hilbert's Theorem 90 ([2], page 323). Let $\alpha \in \mathcal{O}_1$. For some $c \in (R'/M)^\times$ the element $y = c + \alpha\tau_1(c)$ is nonzero since $1, \tau_1$ are linearly independent ([2], page 318). It follows that $\alpha\tau_1(y) = \alpha\tau_1(c) + \alpha\tau_1(\alpha)c = \alpha\tau_1(c) + c = y$. Since $y \neq 0$ we have $\alpha = \frac{y}{\tau_1(y)}$. Now we put $r = y^{-1}$. □

Assume $\tau_1 \neq 1$. Let us consider the element $u_0 \in \mathcal{O}_1$ (in Lemma 2.15). By Theorem 2.17 there exists $r_0 \in (R'/M)^\times$ such that

$$\text{(I)} \qquad r_0^{-1}\tau_1(r_0) = u_0^{-1}.$$

Let $f \in \mathcal{O}_i$. By Theorem 2.16, $f + f_i g^i \in \mathcal{O}_{i+1}$ if and only if $\tau_1(f_i \cdot f_0^{-1})u_0^i + (f_i \cdot f_0^{-1}) = -d_i$. If we replace u_0^{-1} by $r_0^{-1}\tau_1(r_0)$ we obtain $\tau_1(f_i \cdot f_0^{-1}) + (f_i \cdot f_0^{-1})r_0^{-i}\tau_1(r_0^i) = -d_i r_0^{-i}\tau_1(r_0^i)$. So we have

$$\text{(II)} \qquad (\tau_1 + 1)(\frac{f_i}{f_0 \cdot r_0^i}) = -\frac{d_i}{r_0^i}.$$

By (II) and Theorem 2.17 (1) we have $-\frac{d_i}{r_0^i} \in F_1$. Thus a choice for f_i exists only if $\frac{d_i}{r_0^i} \in F_1$. The next lemma shows that this always happens.

LEMMA 2.18. *Suppose that $f \in \mathcal{O}_i$. Let d_i be the ith deviation of f and let r_0 be as in (I). Call $w = \frac{d_i}{r_0^i}$. Then $w \in F_1$.*

PROOF. Since $f \in \mathcal{O}_i$ we have $f \cdot \tau(f) - 1 \equiv d_i g^i \bmod g^{i+1}$. This implies $\tau(f \cdot \tau(f) - 1) \equiv \tau(d_i g^i) \bmod g^{i+1}$. So $f \cdot \tau(f) - 1 \equiv u^i \tau(d_i) g^i \bmod g^{i+1}$, since $\tau^2 = 1$ and $\tau(g) = u \cdot g$. Comparing the congruences above we get $d_i \equiv u^i \tau(d_i) \bmod g$. Thus $d_i = u_0^i \tau_1(d_i)$ where u_0 is the canonical image of u in R'/M. Since $r_0^{-1}\tau_1(r_0) = u_0^{-1}$, we have $\tau_1(w) = \tau_1(\frac{d_i}{r_0^i}) = \frac{d_i}{u_0^i} \cdot \frac{r_0^{-i}}{u_0^{-i}} = w$. $\square$

The next result gives the number of choices for the polynomials f_i that can be used to lift an element $f \in \mathcal{O}_i$ to an element $f + f_i g^i \in \mathcal{O}_{i+1}$, when $\tau_1 \neq 1$.

THEOREM 2.19. *Let* $f \in \mathcal{O}_i$ *and assume* $\tau_1 \neq 1$. *Call* $S_f = \{f_i : f + f_i g^i \in \mathcal{O}_{i+1}\}$. *Then* $|S_f| = |F_1|$.

PROOF. Recall that $(\tau_1 + 1)(\frac{f_i}{f_0 \cdot r_0^i}) = -w$, where $w = \frac{d_i}{r_0^i} \in F_1$. Since f_0, r_0 and w are fixed elements, the only variable is f_i. Let $f_i' = (\frac{f_i}{f_0 \cdot r_0^i})$. Since for any α, $\beta \in R'/M$ the condition $(\tau_1 + 1)(\alpha) = (\tau_1 + 1)(\beta)$ is equivalent to the condition $\alpha \in ker(\tau_1 + 1) + \beta$, by Lemma 2.18 the number of choices for f_i' is equal to $|ker(\tau_1 + 1)|$. Therefore $|S_f| = |ker(\tau_1 + 1)| = |r \cdot F_1| = |F_1|$ (here we used Theorem 2.17 (2)). □

We are assuming that $g \in F[x]$ is an irreducible reciprocal factor of $\psi(x)$ of multiplicity m with degree $2s$. Suppose $\tau_1 \neq 1$. Since τ_1 is a transpose map of $F[x]/(g)$ over F, τ_1 is an automorphism of $F[x]/(g)$ over F_1 of order 2. Let σ be the Frobenius automorphism of $F[x]/(g)$ over F. We have $\tau_1 = \sigma^k$ for some k, $0 \leq k \leq 2s - 1$. Since $\sigma^{2k} = \tau_1^2 = 1$ and the order of σ is $2s$, we have $2s \| 2k$ so $s \| k$. But $k \neq 0$ since $\tau_1 \neq 1$. Therefore $k = s$, that is $\tau_1(z) = z^{q^s}$ for every $z \in F[x]/(g)$. Thus $\mathcal{O}_1 = \{z \in F[x]/(g) : z \cdot z^{q^s} = 1\}$. Since $F[x]/(g) = GF(q^{2s})$ is a finite field, $(F[x]/(g))^\times$ is cyclic and clearly $\mathcal{O}_1$ is its unique multiplicative subgroup of order $q^s + 1$, i.e. $|\mathcal{O}_1| = q^s + 1$. ([2], page 289). Let $G = \{1, \tau_1\}$, then G is a subgroup of automorphisms of the field $F[x]/(g)$. Since F_1 is the fixed field of τ_1, we have $F_1 = GF(q^s)$, ([5], page 483). Let $f = f_0 + f_1 g + f_2 g^2 + \cdots + f_{m-1} g^{m-1} \in \mathcal{O}'$. Since $f_0 \in \mathcal{O}_1$, we have immediately that the number of choices of f_0 is $q^s + 1$. By Theorem 2.19, we have that the number of choices for f_i $(1 \leq i \leq m - 1)$ is $|F_1| = q^s$. Therefore the orthogonal group component $\mathcal{O}'$ corresponding to g has order

$$(**) \qquad |\mathcal{O}'| = (q^s + 1) \cdot q^{s(m-1)}.$$

Example: Let $\psi(x) = x^6 - 1 = (x+1)^2 \cdot (x^2 + x + 1)^2$ over $F = GF(2)$. Let $g = x^2 + x + 1$. Then g is irreducible and reciprocal. We have $R = F[x]/\psi(x) \cong F[x]/(x+1)^2 \oplus F[x]/(g^2)$. Call $R' = F[x]/(g^2)$. The transpose map on R' is a 1-cycle and the corresponding orthogonal group component has order $(q^s + 1) \cdot q^{s(m-1)} = (2^1 + 1) \cdot 2 = 6$.

Now let us suppose $\tau_1 = 1$. By Proposition 2.11, $g = x \pm 1$. Recall that $\tau(g) = u \cdot g$ for some unit u in $R' \cong F[x]/(g^m)$, and that u_0 is the canonical image of u in R'/M, i.e. $u_0 \equiv u \bmod g$. We have

$$\tau(g) = \tau(x \pm 1) = x^{-1} \pm 1 = (\mp 1 + g)^{-1} \pm 1.$$

Since $(-1 + g) \cdot (-1 - g - g^2 - g^3 - \cdots - g^{m-1}) = 1$ and

$$(+1 + g) \cdot (+1 - g + g^2 - g^3 + \cdots + (-1)^{m-1} g^{m-1}) = 1$$

in R', then $\tau(g) = (\mp 1 - g \mp g^2 - g^3 \mp \cdots) \pm 1 = (-1 \mp g - g^2 \mp \cdots)g$. So we have $u = -1 \mp g - g^2 \mp \cdots$ and $u_0 = -1$. Let $1 \leq i \leq m-1$ and let $f = f_0 + f_1 g + f_2 g^2 + \cdots + f_{i-1} g^{i-1} \in \mathcal{O}_i$. By Theorem 2.16, we have that $f + f_i g^i \in \mathcal{O}_{i+1}$ if and only if $\tau_1 (f_i \cdot f_0^{-1}) u_0^i + (f_i \cdot f_0^{-1}) = -d_i$. That is

$$(f_i \cdot f_0^{-1})(1 + (-1)^i) = -d_i.$$

We want to know how to find f_i in R'/M such that $f + f_i g^i \in \mathcal{O}_{i+1}$.

Case (1). If $i \geq 2$ is even and Char$F \neq 2$, then $f_i = -\frac{f_0 d_i}{2}$. (We will discuss the case Char$F = 2$ later).

Case (2). If i is odd then $d_i = 0$. Since $f \in \mathcal{O}_i$ and d_i is the ith deviation of f, we have $f \in \mathcal{O}_{i+1}$. Thus for every $f_i \in R'/M$ we have $f + f_i g^i \in \mathcal{O}_{i+1}$.

If $f \in \mathcal{O}_i$, by the definition of deviation, we have

$$f \cdot \tau(f) - 1 = d_i g^i + d_{i+1} g^{i+1} + \cdots = \sum_{k=i}^{m-1} d_k g^k.$$

Applying τ, we obtain $f \cdot \tau(f) - 1 = \sum_{k=i}^{m-1} d_k (\tau g)^k$. Since $g = x \pm 1$, $\tau(g) = (-1 \mp g - g^2 \mp \cdots)g$, we have

$$f \cdot \tau(f) - 1 = -d_i g^i + (d_{i+1} \mp i \cdot d_i) g^{i+1} + \cdots.$$

Thus

(III) $$d_i = -d_i.$$

(IV) $$i \cdot d_i = 0.$$

If Char$F \neq 2$, $d_i = 0$ by (III). So for every $f_i \in R'/M$ we have $f + f_i g^i \in \mathcal{O}_{i+1}$. Summarizing we obtain the following result: Let $f = f_0 + f_1 g + f_2 g^2 + \cdots + f_{m-1} g^{m-1} \in \mathcal{O}'$ and suppose that Char$F \neq 2$. We have $f_0 \in \mathcal{O}_1 = \{\pm 1\}$, so the number of choices for f_0 is 2; in fact $1 = f_0 \tau_1(f_0) = f_0^2$ if and only if $f_0 = \pm 1$. Let $1 \leq i \leq m-1$. If i is even, $f_i = -\frac{f_0 d_i}{2}$ is a fixed element, if i is odd, then $d_i = 0$. So for f_i we can choose any element in R'/M. Since R'/M has degree 1 over F, the number of choices for f_i is q. Thus we have

THEOREM 2.20. *Suppose that $F = GF(q)$ has characteristic $\neq 2$ and that $g = x \pm 1$ is a factor of $\psi(x)$ of multiplicity m. Then the order of the orthogonal group $\mathcal{O}'$ of $R' = F[x]/(x \pm 1)^m$ is*

$$2 \cdot q^{[\frac{m}{2}]}.$$

If Char$F = 2$ and i is odd, then $d_i = 0$ by (IV). So for every $f_i \in R'/M$ we have $f + f_i g^i \in \mathcal{O}_{i+1}$ (where $f = f_0 + f_1 g + f_2 g^2 + \cdots + f_{i-1} g^{i-1} \in \mathcal{O}_i$). In this case $f_0 \in \mathcal{O}_1 = \{+1\}$ and $g = x + 1$. So $f = 1 + f_1 g \in \mathcal{O}_2$ for every $f_1 \in R'/M$. But if the multiplicity m of g is greater than 2 we have to consider whether or not for such f_1 there exists some $f_2 \in R'/M$ such that $1 + f_1 g + f_2 g^2 \in \mathcal{O}_3$. (It is not true that for every $f_1 \in R'/M$ there exists such f_2).

LEMMA 2.21. *Suppose $f = 1 + f_1 g + f_2 g^2$. Then $f \in \mathcal{O}_3$ if and only if $f_1 = 0$ or $f_1 = 1$.*

PROOF. Since $\tau(g) = (1 + g + g^2 + \cdots)g$, we have $\tau(f) = 1 + f_1 g + (f_1 + f_2)g^2 + \cdots$. Thus

$$f \cdot \tau(f) + 1 = (f_1 + f_1^2)g^2 + \cdots.$$

By Lemma 2.14, $f \in \mathcal{O}_3$ if and only if its 2th deviation is zero, i.e. if and only if $(f_1 + f_1^2) = 0$ in R'/M . Thus $f \in \mathcal{O}_3$ if and only if $f_1 = 0$ or $f_1 = 1$. □

Now let us consider the case $m > 2$. Let $f = 1 + f_1 g + f_2 g^2 + \cdots + f_{i-1} g^{i-1} \in \mathcal{O}_i$, where i is odd and $i \geq 3$. The same problem arises. We have $f + f_i g^i \in \mathcal{O}_{i+1}$

for every $f_i \in R'/M$, but it may happen that does not exist a f_{i+1} such that $f + f_i g^i + f_{i+1} g^{i+1} \in \mathcal{O}_{i+2}$. Suppose $f' = f + f_i g^i + f_{i+1} g^{i+1} \in \mathcal{O}_{i+2}$. Since i is odd we have $f \in \mathcal{O}_{i+1}$; so $f \cdot \tau(f) - 1 \equiv d_{i+1} g^{i+1} \bmod g^{i+2}$. We have that $\tau(f') = \tau(f) + f_i \cdot (\tau(g)^i) + f_{i+1} \cdot (\tau(g))^{i+1}$. Since $\tau(g) = (1 + g + g^2 + \cdots)g$, we can write

$$\tau(f') \equiv \tau(f) + f_i \cdot g^i + (f_i + f_{i+1}) \cdot g^{i+1} \mod g^{i+2}.$$

So

$$f' \cdot \tau(f') \equiv f \cdot \tau(f') + f_i \cdot \tau(f) \cdot g^i + f_{i+1} \cdot \tau(f) \cdot g^{i+1} \mod g^{i+2}.$$

Since $f \cdot \tau(f') = f \cdot \tau(f) + f_i \cdot g^i + (f_i f_1 + f_{i+1} + f_i) g^{i+1} \bmod g^{i+2}$ and $\tau(f) = 1 + f_1 g + (f_1 + f_2) g^2 + \cdots$,
we have

$$f' \cdot \tau(f') = f \cdot \tau(f) + (f_i f_1 + f_{i+1} + f_i f_1 + f_{i+1} + f_i) g^{i+1}.$$

$$= 1 + (f_i + d_{i+1}) g^{i+1}$$

By Lemma 2.14, $f_i + d_{i+1} = 0$ i.e. $f_i = d_{i+1}$. From this we obtain the following theorem.

THEOREM 2.22. *Let $F = GF(q), q = p^l, p = 2$. Suppose that $g = x+1$ is a factor of $\psi(x)$ of multiplicity m. Then the orthogonal group $\mathcal{O}'$ of $R' = F[x]/(x+1)^m$ has order*

$$1 \quad \text{if} \quad m = 1$$

$$q \quad \text{if} \quad m = 2$$

$$2q^{[\frac{m}{2}]} \quad \text{if} \quad m > 2.$$

2-CYCLE CASE.

Now let us look the orthogonal group $\mathcal{O}'$ at a 2-cycle. As at the beginning of this chapter, let g_i and g_j be two nonreciprocal irreducible factors of $\psi(x)$ with the same degree t and multiplicity m and such that $g_i \cdot g_j$ is reciprocal. Call $\mathcal{O}'$ the group of orthogonal elements of $F[x]/(g_i^m) \times F[x]/(g_j^m)$. The transpose map $\tau : F[x]/(g_i^m) \times F[x]/(g_j^m) \longrightarrow F[x]/(g_i^m) \times F[x]/(g_j^m)$ induces an isomorphism between $F[x]/(g_i^m)$ and $F[x]/(g_j^m)$ and $\tau(e_i) = e_j$; thus $\tau \mid_{F[x]/(g_i^m)}$ is inverse to $\tau \mid_{F[x]/(g_j^m)}$. If we identify $F[x]/(g_i^m) \times 0$ with $F[x]/(g_i^m)$, $0 \times F[x]/(g_j^m)$ with $F[x]/(g_j^m)$, then we have $\tau(f_i, f_j) = (\tau(f_j), \tau(f_i))$ where $f_i \in F[x]/(g_i^m)$, $f_j \in F[x]/(g_j^m)$. Since $F[x]/(g_i^m) \times F[x]/(g_j^m) \cong F[x]/((g_i g_j)^m)$ and $\tau^2 = 1$, if f_i is invertible and $f_j = \tau(f_i)^{-1}$, then $(f_i, \tau(f_i)^{-1}) \times \tau(f_i, \tau(f_i)^{-1}) = (1, 1)$, the identity element in $F[x]/(g_i^m) \times F[x]/(g_j^m)$. Therefore $(f_i, \tau(f_i)^{-1}) \in \mathcal{O}'$. Conversely, if some element (f_i, f_j) of $F[x]/(g_i^m) \times F[x]/(g_j^m)$ belongs to $\mathcal{O}'$ then $(1, 1) = (f_i, f_j) \cdot \tau(f_i, f_j) = (f_i, f_j) \cdot (\tau(f_j), \tau(f_i)) = (f_i \cdot \tau(f_j), f_j \cdot \tau(f_i))$, so we have that f_i is invertible and $f_j = \tau(f_i)^{-1}$. Therefore the map π such that

$$\pi : [F[x]/(g_i^m)]^\times \longrightarrow \mathcal{O}'$$

$$f_i \mapsto (f_i, \tau(f_i)^{-1})$$

is an isomorphism from the group of units of $F[x]/(g_i^m)$ to $\mathcal{O}'$. In particular $|\mathcal{O}'| = |(F[x]/(g_i^m))^\times|$. Now, $(F[x]/(g_i^m))^\times = \{f_0 + f_1 g_i + \cdots + f_{m-1} g_i^{m-1} : f_0 \in (F[x]/(g_i))^\times, f_k \in (F[x]/(g_i)) \quad \text{for} \quad 1 \le k \le m-1\}$. Hence $|(F[x]/(g_i^m))^\times| = (q^t - 1) \cdot q^{t(m-1)}$. So we proved the following theorem.

THEOREM 2.23. *Let $F = GF(q)$, $q = p^l$, and g_i, g_j be a 2-cycle pair of factors of $\psi(x)$ (so g_i and g_j are distinct irreducible nonreciprocal and $g_i \cdot g_j$ is reciprocal). Suppose that g_i and g_j have each degree t and multiplicity m. Then the corresponding group $\mathcal{O}'$ of orthogonal elements in $F[x]/(g_i^m) \times F[x]/(g_j^m)$ has order*

$$(q^t - 1) \cdot q^{t(m-1)}.$$

Let us go back to the general situation. Suppose that $\psi(x)$ is the reciprocal polynomial $x^n - 1$. Let $F = GF(q)$, $q = p^l$ and $n = n_1 \cdot p^k$ with $(n_1, p) = 1$. Thus $x^n - 1 = (x^{n_1} - 1)^{p^k}$. Taking derivative for $x^{n_1} - 1$ we have $(x^{n_1} - 1)' = n_1 x^{n_1 - 1}$. Since $(n_1, p) = 1$, we have that $(x^{n_1} - 1)'$ has only zero as a root, but zero is not a root of $x^{n_1} - 1$. Thus $x^{n_1} - 1$ has only simple roots. So, all polynomial factors corresponding to 1-cycles and 2-cycles have the same multiplicity p^k over F.

Let μ_n denote the group of nth roots of unity in the complex field $\mathbb{C}$. If $\varphi(n)$ denotes **Euler**'s ψ-function (= number of integers a, $1 \le a \le n$, relatively prime to n =order of the group $(\mathbb{Z}/n\mathbb{Z})^\times$), then μ_n has $\varphi(n)$ generators. Let ζ_n denote a fixed primitive nth root of unity. Then

$$\mu_n = \{\zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}, \zeta_n^n = 1\}.$$

DEFINITION. *We define the nth cyclotomic polynomial as*

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \zeta primitive}} (x - \zeta) = \prod_{\substack{1 \le a \le n \\ (a,n)=1}} (x - \zeta^a)$$

in $\mathbb{C}[x]$. *It can be shown that* $\Phi_n(x) \in \mathbb{Z}[x]$ *([5], page 466).*

The roots of the polynomial $x^n - 1$ are precisely the nth roots of unity, so we have

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta).$$

If we group together the factors $(x - \zeta)$ where ζ is an element of order d in μ_n (i.e. ζ is a primitive dth root of unity), then we have

$$x^n - 1 = \prod_{d \| n} \prod_{\substack{\zeta \in \mu_d \\ \zeta primitive}} (x - \zeta).$$

Since

$$\Phi_d(x) = \prod_{\substack{\zeta \in \mu_d \\ \zeta primitive}} (x - \zeta),$$

we have

$$x^n - 1 = \prod_{d \| n} \Phi_d(x).$$

Let us consider again the polynomial $x^{n_1} - 1$ defined above. We can factor it as

$$x^{n_1} - 1 = \prod_{d \| n_1} \Phi_d(x) \quad \text{over} \quad F.$$

Let d be a divisor of n_1. Clearly the polynomial $\Phi_d(x)$ is reciprocal. So we can factor $\Phi_d(x)$ into irreducible reciprocal polynomials corresponding to 1-cycles, and pairs of irreducible polynomials (whose product is reciprocal) corresponding to 2-cycles. Let $\Phi_d(x) = g_1 \cdot g_2 \cdots g_k$ be the decomposition of $\Phi_d(x)$ in monic irreducible factors over F, then all the g_i have the same degree. In fact, with $1 \leq i, j \leq k$, let α be a root of g_i and β be a root of g_j in an extension of F, then $F(\alpha) = F(\beta)$ (since $\beta = \alpha^l$ for some l with $(l, d) = 1$). Therefore $\deg(g_i) = [F(\alpha) : F] = [F(\beta) : F] = \deg(g_j)$.

LEMMA 2.24. *Let $\Phi_d(x) = g_1 \cdot g_2 \cdots g_k$ where g_i $(1 \leq i \leq k)$ are irreducible in F, suppose that for some i, g_i is reciprocal with degree $2s$. Then all factors of $\Phi_d(x)$ are reciprocal.*

PROOF. Let τ_1 be the transpose map of $F[x]/(g_i)$. Since τ_1 has order 2 and $F[x]/(g_i) \cong GF(q^{2s})$, τ_1 is the only F-automorphism of order 2 of $GF(q^{2s})$. So $\tau_1(f(x)) = f(x^{-1}) = f(x)^{q^s} = f(x^{q^s})$ for every $f \in F[x]/(g_i)$ and τ_1 inverts every root of g_i. Therefore, if α is a root of g_i then $\alpha \in \mathcal{O}_1 = \{f \in F[x]/(g_i) : f \cdot \tau_1(f) = f^{q^s+1} = 1\}$. So $\alpha^{q^s+1} = 1$, and since α is a primitive dth root of unity, we have $d \| q^s + 1$. Conversely, if $d \| q^s + 1$ for some s, take s minimal. Then $\tau_1(f) = f^{q^s}$ will invert every primitive dth root α of unity thus g_i is reciprocal. Also α has degree $2s$ and so g_i has degree $2s$ over F. Since the fact that $d \| q^s + 1$ is independent of the choice of g_i, all factors of $\Phi_d(x)$ are reciprocal. □

LEMMA 2.25. *Let $\Phi_d(x) = g_1 \cdot g_2 \cdots g_k$ where g_i $(1 \leq i \leq k)$ are irreducible in F, if there exists g_i, for some i, such that g_i is nonreciprocal then all factors of $\Phi_d(x)$ are nonreciprocal.*

PROOF. Immediate, by Lemma 2.24. □

It follows from the proof of Lemma 2.24 that if all the factors of $\Phi_d(x)$ are reciprocal with degree $2s$ then $\Phi_d(x)$ can be factored into $\frac{\varphi(d)}{2s}$ irreducible reciprocal polynomials of $F[x]$, and s is the smallest positive integer such that $d \| q^s + 1$.

Let $\mathbb{Z}_d^\times$ denote the multiplicative group of units of the ring of integers modulo d. Since $(q, d) = 1$, there are $u, v \in \mathbb{Z}$ such that $uq + vd = 1$ thus $uq \equiv 1 \bmod d$. Let $[q]_d$ denote the cyclic subgroup of $\mathbb{Z}_d^\times$ generated by q. We can rewrite the condition of Lemma 2.24 as following.

LEMMA 2.26. *$\Phi_d(x)$ factors into irreducible reciprocal polynomials in $F[x]$ if and only if $-1 \in [q]_d$. In that case every irreducible factor of $\Phi_d(x)$ has degree $|[q]_d|$.*

PROOF. Recall that by Lemma 2.24, $\Phi_d(x)$ factors into irreducible reciprocal polynomials of $F[x]$ if and only if $d \| q^s + 1$ for some s and that these factors have degree $2s$ if we take s minimal. That is, $\Phi_d(x)$ factors into irreducible reciprocal polynomials of degree $2s$ of $F[x]$ if and only if $q^s \equiv -1 \bmod d$ and s is minimal. Suppose that happens. Since $[q]_d$ is the cyclic subgroup of $\mathbb{Z}_d^\times$ generated by q mod d, $q^s \equiv -1 \in [q]_d \bmod d$. Since s is the smallest positive integer such that $q^s \equiv -1$ mod d, s is the smallest such that $q^{2s} \equiv 1 \bmod d$, i.e. $[q]_d$ has order $2s$ which is equal to the degree of the irreducible factors of $\Phi_d(x)$. □

By this Lemma and Lemma 2.25, we have that $\Phi_d(x)$ factors into nonreciprocal irreducible factors in $F[x]$ if and only if $-1 \notin [q]_d$. Since the roots of all factors of $\Phi_d(x)$ are primitive dth roots of unity, every irreducible factor has degree t, where

t is the degree of any primitive dth root of unity over F. Let g be an irreducible factor of $\Phi_d(x)$ and let α be a root of g, since α has degree t over $F = GF(q)$, $\alpha^{q^t-1} = 1$. So $d \| q^t - 1$ and t the smallest such positive integer i.e. t is the smallest positive integer such that $q^t \equiv 1 \bmod d$. Therefore $t = |[q]_d|$.

Now we can state the main theorem, in which we list formulas to count the orders of all orthogonal groups of circulant matrices over $GF(q)$.

THEOREM 2.27. *Let $O_{(n,q)}$ denote the group of orthogonal $n \times n$ circulant matrices over $F = GF(q)$, where $q = p^l$. Write $n = n_1 \cdot p^k$ with $(n_1, p) = 1$. Given a divisor d of n_1, let $h_d = |[q]_d|$, and define $O_d(n,q)$ as follows*

I) For $d = 1, 2$

1) If $p = 2$

$$|O_d(n,q)| = \begin{cases} 1 & \text{if } k = 0 \\ q & \text{if } k = 1 \\ 2 \cdot q^{2^{k-1}} & \text{if } k > 1. \end{cases}$$

2) If $p \neq 2$

$$|O_d(n,q)| = 2 \cdot q^{\frac{1}{2}(p^k-1)}.$$

II) For $d > 2$

1) If $-1 \in [q]_d$

$$|O_d(n,q)| = [(q^{\frac{1}{2}h_d} + 1) \cdot q^{\frac{1}{2}h_d(p^k-1)}]^{\varphi(d)/h_d}.$$

2) If $-1 \notin [q]_d$

$$|O_d(n,q)| = [(q^{h_d}-1)\cdot q^{h_d(p^k-1)}]^{\varphi(d)/2h_d}.$$

Then

$$\boxed{|O_{(n,q)}| = \prod_{d\|n_1} |O_d(n,q)|}.$$

PROOF. Write x^n-1 as $x^n-1=(x^{n_1}-1)^{p^k}$ and factor $x^{n_1}-1$ as $x^{n_1}-1=\prod_{d\|n_1}\Phi_d(x)$ over F, where $\Phi_d(x)$ is the dth cyclotomic polynomial defined above. Then $x^n-1=\prod_{d\|n_1}\Phi_d^{p^k}(x)$ over F. By the definition of $\Phi_d(x)$, $\Phi_{d_1}(x)$ and $\Phi_{d_2}(x)$ are relatively prime if $d_1\neq d_2$, and $\Phi_d(x)$ is reciprocal over F. Therefore we have

$$F[x]/(x^n-1) = \bigoplus_{\substack{d\\ d\|n_1}} F[x]/(\Phi_d^{p^k}(x)).$$

For any fixed divisor d of n_1, let $O_d(n,q)$ denote the group of orthogonal circulants of $F[x]/(\Phi_d^{p^k}(x))$. Then

$$|O_{(n,q)}| = \prod_{d\|n_1} |O_d(n,q)|.$$

It remains to calculate the $|O_d(n,q)|$.

I) For $d=1,2$.

1) If $p=2$, then $\Phi_d(x)=x+1$. By Theorem 2.22 we have that the orthogonal group $O_d(n,q)$ of $F[x]/(x+1)^{p^k}$ has order

$$|O_d(n,q)| = \begin{cases} 1 & \text{if } k=0 \\ q & \text{if } k=1 \\ 2\cdot q^{2^{k-1}} & \text{if } k>1. \end{cases}$$

2) If $p \neq 2$, then p is odd and $\Phi_d(x) = x \pm 1$. By Theorem 2.20, we have the orthogonal group of $F[x]/(x \pm 1)^{p^k}$ has order

$$|O_d(n,q)| = 2 \cdot q^{\frac{1}{2}(p^k-1)}.$$

II) For $d > 2$.

1) If $-1 \in [q]_d$, then, by Lemma 2.26, every irreducible factor of $\Phi_d(x)$ is reciprocal with degree $h_d = |[q]_d|$. Since $\Phi_d(x)$ has degree $\varphi(d)$, $\Phi_d(x)$ can be factored into $\varphi(d)/h_d$ different irreducible reciprocal factors. So by $(*)$, we have

$$|O_d(n,q)| = [(q^{\frac{1}{2}h_d}+1) \cdot q^{\frac{1}{2}h_d(p^k-1)}]^{\varphi(d)/h_d}.$$

2) If $-1 \notin [q]_d$, then, by Lemma 2.25 and 2.26, every irreducible factor of $\Phi_d(x)$ is nonreciprocal with the degree $h_d = |[q]_d|$. Since $\Phi_d(x)$ has degree $\varphi(d)$, $\Phi_d(x)$ can be factored into $\varphi(d)/2h_d$ different polynomial pairs the product of each pair being reciprocal. So by Theorem 2.23 we have

$$|O_d(n,q)| = [(q^{h_d}-1) \cdot q^{h_d(p^k-1)}]^{\varphi(d)/2h_d}.$$

□

Example 1: To find the order of the group of 12×12 orthogonal circulants over $F = GF(2)$.

1) $p = q = 2, n = 12 = 3 \cdot 2^2$ so that $n_1 = 3, k = 2$.

2) The divisors of n_1 are $d = 1, 3$. We have $\varphi(1) = 1$ and $\varphi(3) = 2$.

3) $[q]_1 = [2]_1 = \{1\}, [q]_3 = [2]_3 = \{2,1\} = \{-1,1\}$ so that $h_1 = |[2]_1| = 1, h_2 = |[2]_3| = 2$.

4) $|O_{(12,2)}| = \prod_{d\|3} |O_d(12,2)| = |O_1(12,2)| \cdot |O_3(12,2)|$

$$= (2 \cdot 2^2) \cdot [(2^{\frac{1}{2}2} + 1) \cdot 2^{\frac{1}{2}2(2^2-1)}]^{2/2} = 8 \cdot 3 \cdot 2^3 = \boxed{192}.$$

Example 2: To find the order of the group of 11×11 orthogonal circulants over $F = GF(11)$.

1) $p = q = 11, n = 11$ so that $n_1 = 1, k = 1$.

2) $d = 1$, and $\varphi(1) = 1$.

3) $[q]_d = [11]_1 = \{1\}$ so that $h_1 = |[11]_1| = 1$.

4) $|O_{(11,11)}| = |O_1(11,11)| = 2 \cdot 11^{\frac{1}{2}(11-1)} = \boxed{2 \cdot 11^5}$.

Chapter 3. Construction of the Orthogonal Circulant Matrix Groups $O_{(12,3)}$, $O_{(6,2)}$ and $O_{(14,2)}$.

Compared with the counting $|O_{(n,q)}|$, the method of constructing the elements of $O_{(n,q)}$ is more complicated, as examples in this chapter we construct the orthogonal groups $O_{(12,3)}$, $O_{(6,2)}$ and $O_{(14,2)}$.

Constructing $O_{(12,3)}$.

Since the corresponding polynomial is $x^{12}-1$ and $n = 12 = n_1 \cdot p^k = 4 \cdot 3$, by using the method above we have immediately $|O_{(12,3)}| = \prod_{d|4} |O_d(12,3)| = |O_1(12,3)| \cdot |O_2(12,3)| \cdot |O_4(12,3)| = \boxed{6 \cdot 6 \cdot 36}$. Since we can factor $x^{12}-1 = (x^4-1)^3 = (x+1)^3 \cdot (x-1)^3 \cdot (x^2+1)^3$ where $x \pm 1$ and x^2+1 are irreducible over $F = GF(3)$, and $x \pm 1$ and x^2+1 are 1-cycle polynomials, there are correspondingly three transpose maps τ', τ'' and τ''' on $F[x]/(x+1)^3$, $F[x]/(x-1)^3$ and $F[x]/(x^2+1)^3$ respectively, so that $\mathcal{O} \cong \mathcal{O}' \times \mathcal{O}'' \times \mathcal{O}'''$.

CASE (I). $\mathcal{O}'$

$$\tau' : F[x]/(x+1)^3 \longrightarrow F[x]/(x+1)^3$$

$$\tau'(x) = -x^2$$

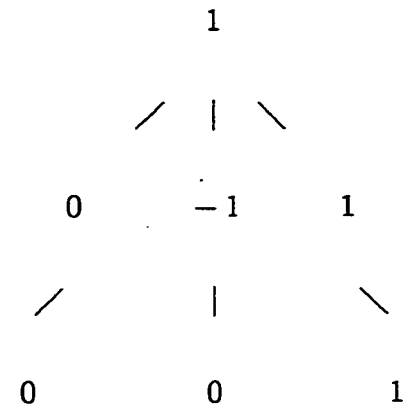
Suppose $f = f_0 + f_1(x+1) + f_2(x+1)^2 \in \mathcal{O}'$, it is easy to see that $f_0 \in \{\pm 1\}$, $f_1 \in \{0, \pm 1\}$. We have to determinate $f_2 = -\frac{d_2 \cdot f_0}{2} = d_2 \cdot f_0$, where d_2 is $f_0 + f_1(x+1)$'s 2th deviation and $d_2 \in F[x]/(x+1) = \{0, \pm 1\}$.

(1) Let $f = 1 + (x+1)$, then $f \cdot \tau'(f) - 1 = (1+x)^2$. Thus $f = 1 + (x+1)$ has 1 as its second deviation i.e. $1 + (x+1) + (x+1)^2 \in \mathcal{O}'$.

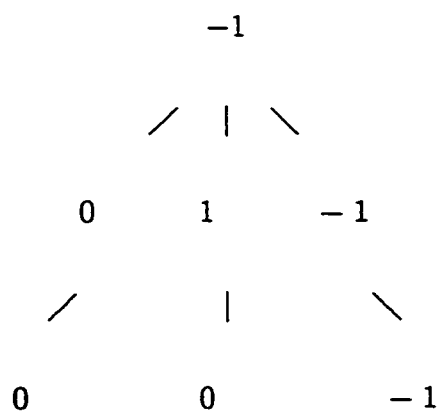
(2) Let $f = 1 - (x + 1)$, then $f \cdot \tau'(f) - 1 = 0$. Thus $f = 1 - (x + 1)$ has 0 as its second deviation i.e. $1 + (x + 1) \in \mathcal{O}'$.

(3) Let $f = 1$, it is obvious that $f = 1$ has 0 as its second deviation thus $f = 1 \in \mathcal{O}'$.

We can write down our results in some simple tree as below



This tree displays the completed the tree for the choice $f_0 = 1$ in $\mathcal{O}'_1$. Since this is the kernel of the canonical map from $\mathcal{O}'$ onto $\mathcal{O}'_1$, the corresponding tree for the choice $f_0 = -1$ can be found by multiplying the tree for $f_0 = 1$ by any one completed path from -1. So we have the tree



CASE (II). $\mathcal{O}''$

$$\tau'' : F[x]/(x-1)^3 \longrightarrow F[x]/(x-1)^3$$

$$\tau''(x) = x^2$$

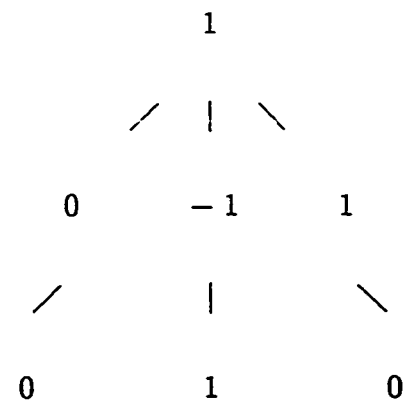
Suppose $f = f_0 + f_1(x-1) + f_2(x-1)^2 \in \mathcal{O}''$, as case (I) we have that $f_0 \in \{\pm 1\}$, $f_1 \in \{0, \pm 1\}$ and we will determinate $f_2 = -\frac{d_2 \cdot f_0}{2} = d_2 \cdot f_0$, where d_2 is $f_0 + f_1(x-1)$'s 2th deviation and $d_2 \in F[x]/(x+1) = \{0, \pm 1\}$.

(1) Let $f = 1 + (x-1)$, then $f \cdot \tau'(f) - 1 = 0$. Thus $f = 1 + (x-1)$ has 0 as its second deviation i.e. $1 + (x-1) \in \mathcal{O}''$.

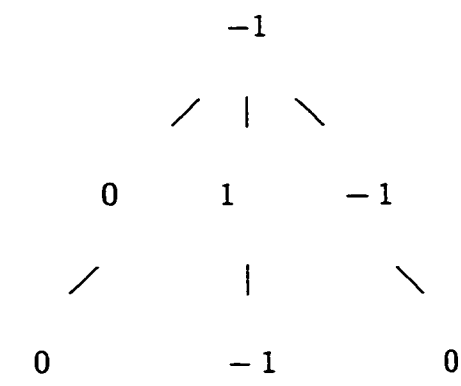
(2) (1) Let $f = 1 - (x-1)$, then $f \cdot \tau'(f) - 1 = (x-1)^2$. Thus $f = 1 - (x-1)$ has -1 as its second deviation i.e. $1 - (x-1) + (x-1)^2 \in \mathcal{O}''$.

(3) Let $f = 1$, it is obvious that $f = 1$ has 0 as its second deviation thus $f = 1 \in \mathcal{O}''$.

We can write down our results in some simple tree as below



Similarly as Case(I), we can construct the tree for $f_0 = -1$ as



CASE (III). $\mathcal{O}'''$

$$\tau''' : F[x]/(x^2+1)^3 \longrightarrow F[x]/(x^2+1)^3$$

$$\tau'''(x) = x^{-1} = -x^5$$

Since the multiplicity of $g(x) = x^2+1$ is $m = 3$, we can suppose that $f = f_0 + f_1 \cdot g + f_2 \cdot g^2 \in \mathcal{O}'''$ so that we have to find f_0, f_1 and f_2. By (II) we have if $\tau_1 \neq 1$ then $(\tau_1+1)(\frac{f_i}{f_0 \cdot r_0^i}) = -\frac{d_i}{r_0^i}$. We will use (II) to find f_1 and f_2.

LEMMA 3.1. *Let τ be a transpose map of $F[x]/(g^m)$ where g is an irreducible reciprocal factor of $\psi(x)$ as before. Suppose $\tau_1 \neq 1$ and $f = f_0 + f_1 \cdot g + f_2 \cdot g^2 + \cdots + f_{m-1} \cdot g^{m-1} \in \mathcal{O}$ then there exists an element α of R/M such that $f_i \in f_0 \cdot r_0^i(\alpha + F_1)$ mod g for $1 \leq i \leq m-1$.*

PROOF. By (II), let α be an element of R/M such that $(\tau_1+1)(\alpha) = -\frac{d_i}{r_0^i}$. Comparing it with (II) we have $f_i/(f_0 \cdot r_0^i) - \alpha \in Ker(\tau_1+1) = F_1$. Thus $f_i \in f_0 \cdot r_0^i(\alpha + F_1)$. $\square$

From this lemma, in order to find f_i it is enough to find α, f_0, F_1 and r_0. Since α is an element of the field (finite) of R/M, $f_0 \in \mathcal{O}_1$ and F_1 is the fixed field of $(\tau_1 + 1)$ in R/M, we have that α, f_0, F_1 and r_0 are relatively easy to find. The next lemma giving a way to determinate the remaining element r_0.

LEMMA 3.2. *If $R' = F[x]/(g^m)$, where g is an irreducible reciprocal polynomial of degree $2s$, then we may take $r_0 = x^{-s}$ mod g.*

PROOF. Let $\overline{F}$ denote the splitting field of $g(x)$ over F. Then we have corresponding the ring $\overline{R}' = \overline{F}[x]/(g^m)$ which contains R'. We suppose $\overline{\tau}$ which is the transpose map of $\overline{R}'$. Since g is irreducible reciprocal polynomial of $F[x]$ with degree $2s$, in $\overline{F}[x]$ we can write g as $g = \prod_{i=1}^{s}(x - \alpha_i)(x - \alpha_i^{-1})$ where α_j and α_k are not mutually reciprocal if $j \neq k$ for $1 \leq j, k \leq s$. So $\tau(g) = \overline{\tau}(g) = \prod_{i=1}^{s}(x^{-1} - \alpha_i)(x^{-1} - \alpha_i^{-1})$. Multiplying $\tau(g)$ by x^{2s} we have $x^{2s}\tau(g) = \prod_{i=1}^{s}(1 - \alpha_i x)(1 - \alpha_i^{-1}x) = \prod_{i=1}^{s}(x - \alpha_i)(x - \alpha_i^{-1})$ in $\overline{F}[x]$. Since $\tau(g) = u \cdot g$ for some unit u in R' and $u = u_0$ mod g, we have $u_0 \equiv x^{-2s}$ mod g. Taking $r_0 \equiv x^{-s}$ mod g we have $r_0^{-1}\tau_1(r_0) = x^s\tau_1(x^s) = x^{2s} \equiv u_0^{-1}$ mod g which satisfies (I). □

By Lemma 3.2 for the ring $F[x]/(x^2 + 1)^3$ we can take $r_0 \equiv x^{-1} \equiv -x$ mod $(x^2 + 1)$. In general for the ring $F[x]/(g^m)$, if the degree and the multiplicity (m) of g are relatively small number, then we can always find r_0 directly. In particular for $F[x]/(x^2+1)^3$, we have $\tau'''(x^2+1) \equiv u(x^2+1)$ mod $(x^2+1)^3$ for some unit u in $F[x]/(x^2+1)^3$ then $x^{-2}+1 \equiv u(x^2+1)$ mod $(x^2+1)^3$ so that $x^{-2}(x^2+1) \equiv u(x^2+1)$ mod $(x^2 + 1)$. Thus

$$u \equiv x^{-2} \mod (x^2+1)^2$$

i.e. $u \equiv 2x^2 + 1 \bmod (x^2+1)^2$. It follows that

$$u \equiv u_0 \equiv -1 \mod (x^2+1).$$

We take $r_0 \equiv x^{-1} \equiv -x \bmod (x^2+1)$ then $r_0^{-1} \cdot \tau'''(r_0) \equiv x \cdot \tau'''(x^{-1}) \equiv x^2 \equiv -1 \equiv u_0 \bmod (x^2+1)$ which satisfies (I).

Now let us consider the transpose map $\tau''' : F[x]/(x^2+1)^3 \longrightarrow F[x]/(x^2+1)^3$. Since x^2+1 has degree 2 over $F = GF(3)$, $\mathcal{O}_1'''$ is orthogonal subgroup of the group $[F[x]/(x^2+1)]^\times$ which has order $q^s + 1 = 3 + 1 = 4$ where q is the order of F, s is degree of (x^2+1) divied by 2. So $\mathcal{O}_1''' = \{\pm 1, \pm x\}$ then we have $f_0 \in \{\pm 1, \pm x\}$. By Lemma 3.1 we can take $\alpha = \frac{d_i}{r_0^i}$ so that $f_i \in f_0(d_i + r_0^i F_1) = f_0(d_i + (-x)^i F)$ $(**)$ for $i = 1, 2$ where $F_1 = F = GF(3)$.

We take $f_0 = 1$, let $f = f_0 = 1 \in \mathcal{O}_1'''$ then it is easy to see that the first deviation of $f = f_0$ is zero so that by $(**)$, we have $f_1 \in \{\pm x, 0\}$. Since $\tau'''(x) = -x^5 = -x - xg - xg^2$, $\tau'''(x^2) = \tau'''(x)^2 = -1 - g - g^2$. Thus

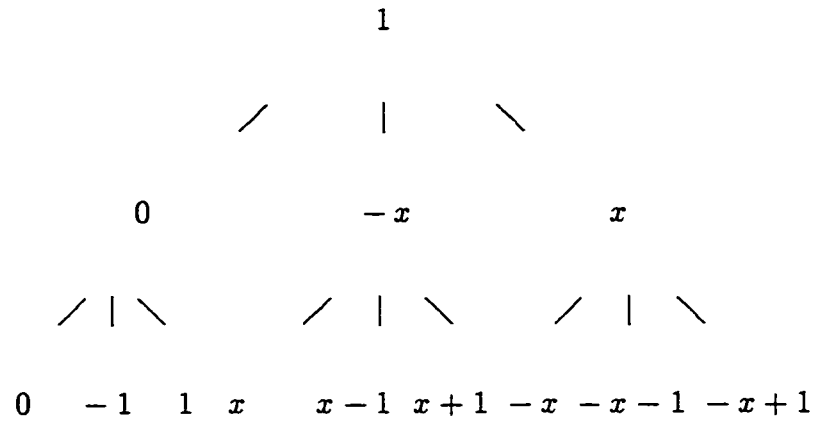
$$\tau'''(g) = \tau'''(x^2+1) = -g - g^2 g$$

Let $f = f_0 + f_1 g = 1 + xg \in \mathcal{O}_2'''$, in order to find f_2, such that $f + f_2 g^2 \in \mathcal{O}'''$ we have to calculate its the second deviation. Since $\tau'''(f) = 1 + \tau'''(x) \cdot \tau'''(g) = 1 + xg - xg^2$, $f \cdot \tau'''(f) = (1+xg)(1+xg-xg^2) = 1 - xg - (1+x)g^2$. So that f has $-(1+x)$ as its the second deviation. Thus $f_2 \in [-(1+x) - F] = \{-x, -(x \pm 1)\}$.

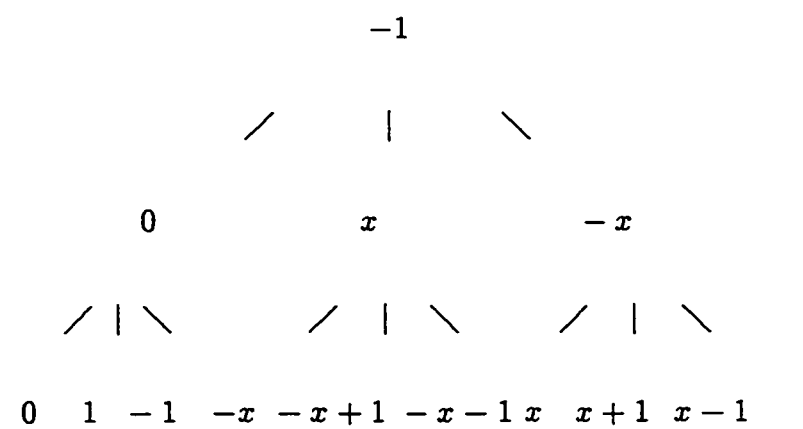
Let $f = f_0 + f_1 g = 1 - xg \in \mathcal{O}_2'''$, we have $f \cdot \tau'''(f) = (1 - xg)(1 - xg + xg^2) = 1 + xg + (x-1)g^2$. So that f has $(x-1)$ as its the second deviation. Thus $f_2 \in [(x-1) - F] = \{x, x \pm 1\}$.

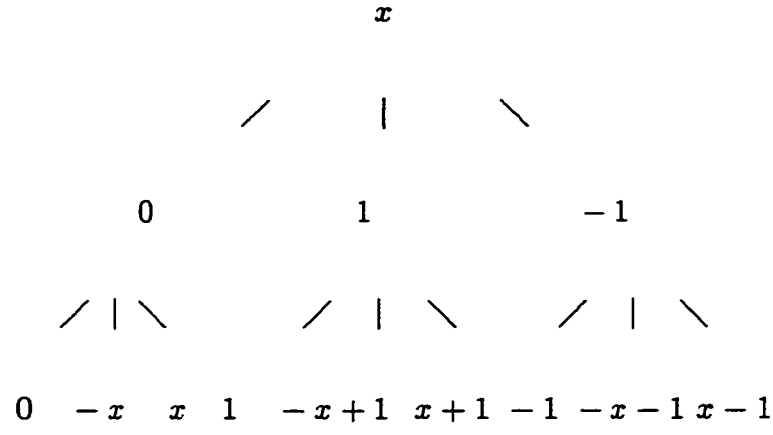
Let $f = f_0 + f_1 g = 1 + 0g \in \mathcal{O}_2'''$, we have $f \cdot \tau'''(f) = 1$ so that f has zero as its the second deviation. Thus $f_2 \in -F = \{0, \pm 1\}$.

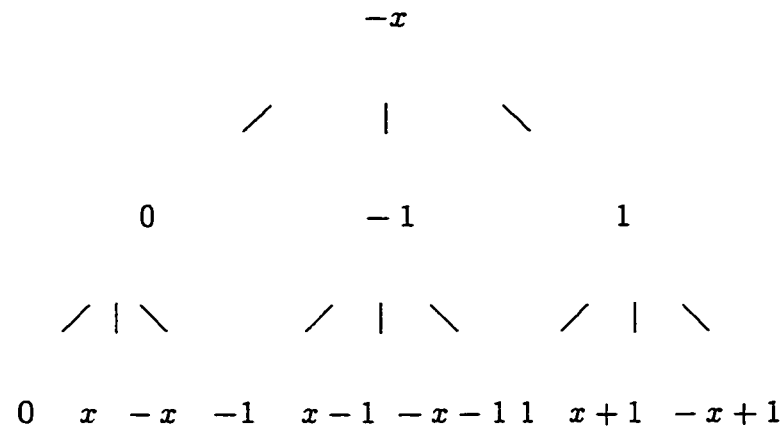
We use a simple tree to express our result as follows



This tree displays the completed the tree for the choice $f_0 = 1$ in $\mathcal{O}_1'''$. Since this is the kernel of the canonical map from $\mathcal{O}'''$ onto $\mathcal{O}_1'''$, the corresponding trees for the choice $f_0 = -1, f_0 = x$, and $f_0 = -x$ can be found by multiplying the trees for $f_0 = 1$ by any one completed path from $-1, x$ and $-x$ correspondingly. So we have the trees







Now we have got all elements for the groups of orthogonal circulants $\mathcal{O}', \mathcal{O}''$ and $\mathcal{O}'''$. Recall that Theorem 2.27, we write $x^n - 1 = (x^{n_1} - 1)^{p^k}$ with $(n_1, p) = 1$ over F then we have

$$F[x]/(x^n - 1) = \oplus \sum_{\substack{d \\ d|n_1}} F[x]/(\Phi_d^{p^k}(x)).$$

Let K be the set such that $D = \{d : \quad d|n_1\}$. For any fixed such d let e_d is an idempotent of $F[x]/(\Phi_d^{p^k}(x))$ and let $\xi = \{e_d : \quad d|n_1\}$. Then

$$F[x]/(x^n-1) = \oplus \sum_{\substack{d \\ d|n_1}} e_d \frac{F[x]/}{(\Phi_d^{p^k}(x))}. \quad (***)$$

Let τ be a transpose map of $F[x]/(\Phi_d^{p^k}(x))$, an orbit of τ in ξ is a set of the form $\xi_d = \{e_d, \tau(e_d)\}$ such that ξ_d are all the distinct orbits, let $\Im_k = \oplus_{e \in \xi_d} e\frac{F[x]}{(x^n-1)}$ be the ideal generated by a given orbit ξ_d which is a direct sum of the ring $e\frac{F[x]}{(x^n-1)}$, then the transpose map τ of $F[x]/(x^n-1)$ acts on each $\Im_d$ as an automorphism by restriction. So that $\mathcal{O} \cong \prod_{d \in D} \mathcal{O}\,|_{\Im_d}$ $(****)$. By $(***)$ and $(****)$, in order to construct the elements of $F[x]/(x^n-1)$ it is enough to find each e_d. For the ring $F[x]/(x^{12}-1)$, let e_1, e_2 and e_3 denote the idempotents of $F[x]/(x+1)^3, F[x]/(x-1)^3$ and $F[x]/(x^2+1)^3$ correspongingly then by Theorem 3.5 we suppose that $e_1 \equiv (x-1)^3(x^2+1)^3 h_1 \bmod (x+1)^3$, $e_2 \equiv (x+1)^3(x^2+1)^3 h_2 \bmod (x-1)^3$ and $e_3 \equiv (x-1)^3(x+1)^3 h_1 \bmod (x^2+1)^3$ also $h_1(x-1)^3(x^2+1)^3 \equiv 1 \bmod (x+1)^3$, $h_2(x+1)^3(x^2+1)^3 \equiv 1 \bmod (x-1)^3$ and $h_3(x+1)^3(x-1)^3 \equiv 1 \bmod (x^2+1)^3$. By Eucliden algorithm we get

$$e_1 \equiv -(x-1)^3(x^2+1)^3 \quad \bmod(x^{12}-1)$$

$$e_2 \equiv (x+1)^3(x^2+1)^3 \quad \bmod(x^{12}-1)$$

$$e_3 \equiv (x-1)^3(x+1)^3 \quad \bmod(x^{12}-1).$$

As an example, we construct an element in $\mathcal{O}$ of $F[x]/(x^{12}-1)$. Take path $(1,1,1)$ in $\mathcal{O}'$, $(1,-1,1)$ in $\mathcal{O}''$ and $(1,0,0)$ in $\mathcal{O}'''$ we have $e_1(1,1,1)+e_2(1,-1,1)+e_3(1,0,0) \in \mathcal{O}$ i.e. $-(x-1)^3(x^2+1)^3[1+(x+1)+(x+1)^2]+(x+1)^3(x^2+1)^3[1-$

$(x-1)+(x-1)^2]+(x-1)^3(x+1)^3 = -1-x^2+x^6-x^8$. This implies a circulant of $O_{(12,3)}$ whose first row is $(-1,0,-1,0,0,0,1,0,-1,0,0,0)$.

Constructing $O_{(6,2)}$.

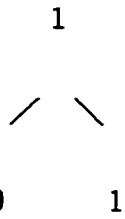
Since the corresponding polynomial is x^6-1 and $6 = 3 \times 2$, by Theorem 2.27 we have $|O_{(6,2)}| = \Pi_{d|3}\,|O_d(6,2)|$ for $1 \leq d \leq 3$. Therefore $|O_{(6,2)}| = |O_1(6,2)| \cdot |O_3(6,2)| = 2\cdot[(2+1)\cdot 2] = 12$. Since $x^6-1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$ over $\mathbb{Q}$, we obtain $x^6+1 = (x+1)^2(x^2+x+1)^2$ over $F = GF(2)$. Call $\mathcal{O} \cong \mathcal{O}' \times \mathcal{O}''$ where $\mathcal{O}$, $\mathcal{O}'$ and $\mathcal{O}''$ are corresponding orthogonal groups of $F[x]/(x^6+1)$, $F[x]/(x+1)^2$ and $F[x]/(x^2+x+1)^2$. Suppose that τ' is the transpose map of $F[x]/(x+1)^2$, τ'' is the transpose map of $F[x]/(x^2+x+1)^2$.

CASE (I). $\mathcal{O}'$

$$\tau' : F[x]/(x+1)^2 \longrightarrow F[x]/(x+1)^2$$

$$\tau'(x) = x$$

Suppose $f = f_0 + f_1(x+1) \in \mathcal{O}'$, by Theorem 2.20 and Lemma 2.21 we have $f_0 = 1$, $f_1 \in \{0,1\}$. Thus the set $\mathcal{O}'$ can be displayed as a tree



i.e. $\mathcal{O}' = \{1, 1+(x+1)\}$.

CASE (II). $\mathcal{O}''$

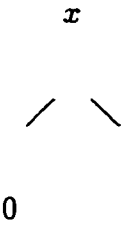
$$\tau'' : F[x]/(x^2+x+1)^2 \longrightarrow F[x]/(x^2+x+1)^2$$

$$\tau''(x) = x^3 + x$$

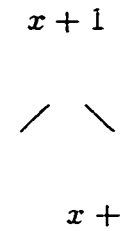
Suppose $f = f_0 + f_1(x+1) \in \mathcal{O}''$. It is clear that $\mathcal{O}''_1$ is the multiplicative group $[F[x]/(x^2+x+1)]^\times = [GF(4)]^\times = \{1, x, x+1\}$. i.e. $f_0 \in \{1, x, x+1\}$. We have to find $f_1 \in F[x]/(x^2+x+1)$ such that $f = f_0 + f_1(x+1) \in \mathcal{O}''$. By Lemma 3.2 we can take $r_0 = x+1$, let $\alpha = d_i x/r_0$ then $\alpha \in F[x]/(x^2+x+1)$ and it is esay to see that $(\tau''_1 + 1)(\alpha) = d_i/r_0$. So that by Lemma 3.1 we have $f_1 \in f_0 r_0(d_1 x/r_0 + F_1) = f_0(d_1 x + F_1)$ where $F_1 = F = GF(2)$. If $f_0 = 1$, we find the first deviation of $f = f_0 = 1$ is zero, so $f_1 \in r_0 F_1 = \{0, x+1\}$. Thus for $f_0 = 1$ the set in $\mathcal{O}''$ can be displayed as a tree

$$\begin{array}{ccc} & 1 & \\ & / \quad \backslash & \\ 0 & & x+1. \end{array}$$

For $f_0 = x$ the set in in $\mathcal{O}''$ is the tree of the tree for $f_0 = 1$ multiplying by x that is



Similarly for $f_0 = x + 1$ we have tree



As example 1, to find the elements of $\mathcal{O}$ we have to find the idempotents of $F[x]/(x^6+1)$. Let e_1, e_2 be the idempotents of $F[x]/(x+1)^2$ and $F[x]/(x^2+x+1)^2$ respectively. Suppose that

$$e_1 \equiv (x^2+x+1)^2 h_1 \equiv 1 \mod (x+1)^2$$

$$e_2 \equiv (x+1)^2 h_2 \equiv 1 \mod (x^2+x+1)^2.$$

By the Eucliden algorithm we have

$$e_1 \equiv (x^2+x+1)^2 \mod (x^6+1)$$

$$e_2 \equiv (x+1)^2 x^2 \mod (x^6+1).$$

Take path $(1,0)$ in $\mathcal{O}'$, $(1,x+1)$ in $\mathcal{O}''$, we obtain $e_1(1,0)+e_2(1,x+1)=1+x+x^2+x^3+x^4 \in \mathcal{O}$. This implies that a circulant matrix of $O_{(6,2)}$ whose first row is $(1,1,1,1,1,0)$. Then 12 of 6×6 orthogonal circulant matrices over $F=GF(2)$ with the first rows are

$$\begin{array}{ll} (1,0,0,0,0,0) & (1,1,1,1,1,0) \\ (0,1,0,0,0,0) & (0,1,1,1,1,1) \\ (0,0,1,0,0,0) & (1,0,1,1,1,1) \\ (0,0,0,1,0,0) & (1,1,0,1,1,1) \\ (0,0,0,0,1,0) & (1,1,1,0,1,1) \\ (0,0,0,0,0,1) & (1,1,1,1,0,1) \end{array}$$

Constructing $O_{(14,2)}$.

Since the corresponding polynomial is $x^{14}-1$ and $14=7\times 2$, by Theorem 3.27 we have $|O_{(14,2)}| = \Pi_{d|7}|O_d(6,2)|$ for $1 \le d \le 7$. Then $|O_{(14,2)}| = |O_1(14,2)| \cdot |O_7(14,2)| = 2\cdot 56 = 112$. Write $x^{14}-1=(x+1)^2(x^3+x+1)^2(x^3+x^2+1)^2$ over $F=GF(2)$ where $x+1$, x^3+x+1 and x^3+x^2+1 are irreducible over F. Let α be a root of x^3+x+1 then α^{-1} is a root of x^3+x^2+1. By the definition we have that x^3+x+1 and x^3+x^2+1 are not reciprocal but the product of them is reciprocal. Call $\mathcal{O} \cong \mathcal{O}' \times \mathcal{O}''$ where $\mathcal{O}$, $\mathcal{O}'$ and $\mathcal{O}''$ are corresponding orthogonal groups of $F[x]/(x^{14}+1)$, $F[x]/(x+1)^2$ and $F[x]/(x^3+x+1)^2 \times F[x]/(x^3+x^2+1)^2$. Suppose that τ' is the transpose map of $F[x]/(x+1)^2$, τ'' is the transpose map of $F[x]/(x^3+x+1)^2 \times F[x]/(x^3+x^2+1)^2$.

CASE (I). $\mathcal{O}'$

The same as $\mathcal{O}'$ of $O_{(6,2)}$, we have $\mathcal{O}' = \{1, 1+(x+1)\}$.

CASE (II). $\mathcal{O}''$

$$\tau'' : F[x]/(x^3+x+1)^2 \longrightarrow F[x]/(x^3+x^2+1)^2$$

$$\tau''(x) = x^5 + x^3$$

The multiplicative group of $[F[x]/(x^3+x+1)]^\times = [GF(2^3)]^\times = \{1, x, x+1, x^2, x^2+1. x^2+x, x^2+x+1\}$. Suppose $f = f_0 + f_1(x^3+x+1) \in F[x]/(x^3+x+1)^2$ then f is a unit of $F[x]/(x^3+x+1)^2$ if and only if $f_0 \in \{1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ and $f_1 \in \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$. By Theorem 3.23 then $\mathcal{O}'' = \{f \times \tau''(f)^{-1} : \text{ for all units } f \in F[x]/(x^3+x+1)^2\}$. As before let e_1, e_2 and e_3 be the idempotents of $F[x]/(x+1)^2$, $F[x]/(x^3+x+1)^2$ and $F[x]/(x^3+x^2+1)^2$ respectively. Suppose that

$$e_1 \equiv (x^3+x+1)^2(x^3+x^2+1)^2 h_1 \equiv 1 \mod (x+1)^2$$

$$e_2 \equiv (x+1)^2(x^3+x^2+1)^2 h_2 \equiv 1 \mod (x^3+x+1)^2$$

$$e_3 \equiv (x+1)^2(x^3+x+1)^2 h_3 \equiv 1 \mod (x^3+x^2+1)^2.$$

By the Eucliden algorithm we have

$$e_1 \equiv (x^3+x+1)^2(x^3+x^2+1)^2 \equiv 1 \mod (x^{14}+1)$$

$$e_2 \equiv (x+1)^2(x^3+x^2+1)^2 \equiv 1 \mod (x^{14}+1)$$

$$e_3 \equiv (x+1)^2(x^3+x+1)^2(x^4+1) \equiv 1 \qquad \mod \quad (x^{14}+1).$$

Take $1 \in \mathcal{O}'$ and $f = 1 + x(x^3+x+1)$ the unit of $F[x]/(x^3+x+1)^2$, since $\tau''(f) = x^5+x^4+x^3 = 1+(x^2+1)(x^3+x^2+1)$, we have $\tau''(f)^{-1} = x^5+x^4+x^3$ in $F[x]/(x^3+x^2+1)^2$. Therefore $(x^3+x+1)^2(x^3+x^2+1)^2 + (x+1)^2(x^3+x^2+1)^2[1+x(x^3+x+1)] + (x+1)^2(x^3+x+1)^2(x^4+1)(x^5+x^4+x^3) = 1+x+x^3+x^4+x^6+x^8+x^{10}+x^{11}+x^{13}$. This implies a 14×14 orthogonal circulant matrix with first row $(1,1,0,1,1,0,1,0,1,0,1,1,0,1)$ over $F = GF(2)$.

Chapter 4. Normal and Normal Orthogonal Bases over Finite Fields.

Our purpose in this section is to investigate the relations between any two normal bases and between any two normal orthogonal bases, as well as the existence of normal orthogonal basis for an extension field K/F and the number of normal orthogonal bases for K/F when one exists.

DEFINITION. *Let K/F be a finite Galois extension of degree n. Let $G = \{\sigma_1, \sigma_2, \cdots,$ be its Galois group. A basis B of K/F is called a normal basis if*
$B = \{\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_n(\alpha)\}$ *for some* $\alpha \in K$.

THEOREM 4.1. *Let K/F be a finite Galois extension of degree n, let $G = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ be its Galois group. Then there exists an element $\alpha \in K$ such that*
$\{\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_n(\alpha)\}$ *is a normal basis of K over F (see [2] Theorem 13.1, or [11] Lemma 3).*

Let K/F be a finite *Galois* extension and let G be its *Galois* group. For $\beta \in K$, we define the *trace* of β relative to K/F as

$$tr_{K/F}(\beta) = \sum_{\sigma \in G} \sigma(\beta).$$

DEFINITION. *A normal basis $B = \{\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_n(\alpha)\}$ is called a normal orthogonal basis if*

$$tr_{K/F}(\sigma_i(\alpha) \cdot \sigma_j(\alpha)) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Let us assume now that $F = GF(q)$, with $q = p^m$, p prime, let $K = GF(q^n)$ (a finite extension of F with degree n). The corresponding *Galois* group G of K/F is then a cyclic group of order n generated by the *Frobenius* automorphism $\sigma : x \mapsto x^q$. So we can redefine a normal basis of K/F as a basis B such that $B = \{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ for some $\alpha \in K$.

LEMMA 4.2. *Let $F = GF(q)$ with $q = p^m$, let $K = GF(q^n)$ be a finite extension of F with degree n. Then*

(1) $tr_{K/F}(\beta) \in F, \qquad \beta \in K$

(2) $tr_{K/F}(\beta^q) = tr_{K/F}(\beta), \qquad \beta \in K$

(3) $tr_{K/F}(a\beta + b\gamma) = a \cdot tr(\beta) + b \cdot tr(\gamma), \qquad \beta, \gamma \in K, \quad a, b \in F.$

PROOF. (1) Let $\beta \in K$, then the trace of β relative to K/F is the sum of the conjugates of β with respect to K/F. Suppose that $f(x) \in F[x]$ is the minimal polynomial of β over F with degree d, then d is a divisor of n and $\beta, \beta^q, \cdots, \beta^{q^{d-1}}$ are the distinct roots of $f(x)$ in K. Let $g(x) = f(x)^{n/d}$, then $g(x)$ has degree n and has also $\beta, \beta^q, \cdots, \beta^{q^{d-1}}$ as its the distinct roots, and each repeated n/d times. This implies that the roots of $g(x)$ in K are precisely the conjugates of β with respect to K/F. i.e. $\beta, \beta^q, \cdots, \beta^{q^{n-1}}$. Hence we have that

$$g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \beta)(x - \beta^q) \cdots (x - \beta^{q^{n-1}}),$$

where $a_i \in F$, $0 \leq i \leq n - 1$. A comparison of coefficients shows that

$$tr_{K/F}(\beta) = -a_{n-1}.$$

(2) and (3) are obvious. □

Note: For a matrix $A = (a_{ij})$, $tr_{K/F}(A)$ means the matrix with $tr_{K/F}(a_{ij})$ as its (i,j)th element.

We start our discussion with a simple example.

Let $F = GF(5)$. The field $F(\sqrt{2})$ is the splitting field of the minimal polynomial $x^2 - 2$ over F, and $F(\sqrt{2})$ has degree 2 over F. It is clear that $1, \sqrt{2}$ is a basis of $F(\sqrt{2})$ but it is not a normal basis. Let $\beta_1 = 1 + \sqrt{2} \in F(\sqrt{2})$ then $\beta_2 = \beta_1^5 = 1 - \sqrt{2} \in F(\sqrt{2})$. It is easy to check that β_1, β_2 is a basis of $F(\sqrt{2})$ so, by definition, it is a normal basis. Similarly $\alpha_1 = 2 + \sqrt{2}, \alpha_2 = 2 - \sqrt{2}$ is another normal basis of $F(\sqrt{2})$. Since $\alpha_1 = -\beta_1 + 3\beta_2$ and $\alpha_2 = 3\beta_1 - \beta_2$, the transformation matrix from the basis (β_1, β_2) to (α_1, α_2) is

$$\begin{pmatrix} -1 & 3 \\ 3 & -1 \end{pmatrix},$$

a circulant matrix with entries in F.

In general, let K be a *Galois* extension of $F = GF(q)$ with degree n and let $B = \{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ and $B' = \{\beta, \beta^q, \cdots, \beta^{q^{n-1}}\}$ be two normal bases of K/F, then there exist n unique elements $a_0, a_1, \cdots, a_{n-1}$ in F such that

$$\alpha = a_0\beta + a_1\beta^q + \cdots + a_{n-1}\beta^{q^{n-1}}$$

where $a_i \neq 0$ for some i, $0 \leq i \leq n-1$. Applying powers of the *Frobenius* automorphism σ for α. We obtain

$$\alpha = a_0\beta + a_1\beta^q + \cdots + a_{n-1}\beta^{q^{n-1}}$$

$$\alpha^q = a_{n-1}\beta + a_0\beta^q + \cdots + a_{n-2}\beta^{q^{n-1}}$$

$$\vdots$$

$$\alpha^{q^{n-1}} = a_1\beta + a_2\beta^q + \cdots + a_0\beta^{q^{n-1}}.$$

So, the transformation matrix from the basis B' to B is

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ . & . & . & . \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}.$$

We find that A is a circulant matrix.

Now we investigate the transformation matrix between any two normal **orthogonal** bases of K/F.

THEOREM 4.3. *Let $F = GF(q)$, $q = p^m$. Let $K = GF(q^n)$ be a finite extension of F. Then K/F has a normal orthogonal basis if and only if n is odd or $n \equiv 2$ mod 4 and q is even (see [11], page 193).*

From this theorem we know that it is not true that there always exists a normal orthogonal basis for a *Galois* extension K/F.

LEMMA 4.4. *For $1 \leq i, j \leq n$, let $A = (a_{ij})$ be a $n \times n$ matrix with entries in F and let $B = (\alpha_{ij})$ be a $n \times n$ matrix with entries in K . Then $tr_{K/F}(A \cdot B) = A \cdot tr_{K/F}(B)$.*

PROOF. Suppose that $A \cdot B = C = (c_{ij})$ then $c_{ij} = \sum_{k=1}^{n} a_{ik}\alpha_{kj}$. We have $tr_{K/F}(A \cdot B) = (tr_{K/F}(c_{ij}))$. By Lemma 4.2 we obtain $tr_{K/F}(c_{ij}) = tr_{K/F}(\sum_{k=1}^{n} a_{ik}\alpha_k$ $= (\sum_{k=1}^{n} a_{ik} tr_{K/F}(\alpha_{kj}))$ the i, j element of $A \cdot tr_{K/F}(B)$. □

THEOREM 4.5. *Let $F = GF(q)$, $q = p^m$. Let $K = GF(q^n)$ be a Galois extension of F with degree n. Suppose that $B = \{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ and $B' = \{\beta, \beta^q, \cdots, \beta^{q^{n-1}}\}$ are two normal orthogonal bases of K/F, then the transformation matrix between B and B' is an orthogonal circulant matrix with entries in F.*

PROOF. As above, let

$$\alpha = a_0\beta + a_1\beta^q + \cdots + a_{n-1}\beta^{q^{n-1}}$$

then the transformation matrix from B' to B is

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}.$$

We have to prove that A is orthogonal. i.e. $A \cdot A^T = I$. Let β' denote the row vector $(\beta, \beta^q, \cdots, \beta^{q^{n-1}})$ and let α' denote the row vector $(\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}})$, then

$$\alpha' = \beta' \cdot A^T, \qquad (\alpha')^T = A \cdot (\beta')^T.$$

So that

$$(\alpha')^T \cdot \alpha' = A \cdot ((\beta')^T \beta') \cdot A^T,$$

where $(\alpha')^T \cdot \alpha'$ is the $n \times n$ matrix with i-th row $\alpha^{q^i}(\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}})$ and $(\beta')^T\beta'$ is the $n \times n$ matrix with i-th row $\beta^{q^i}(\beta, \beta^q, \cdots, \beta^{q^{n-1}})$. Applying tr, we have

$$tr_{K/F}((\alpha')^T \cdot \alpha') = tr_{K/F}(A \cdot ((\beta')^T\beta') \cdot A^T).$$

By Lemma 4.4 we have

$$tr_{K/F}((\alpha')^T \cdot \alpha') = A \cdot (tr_{K/F}((\beta')^T \beta')) \cdot A^T. \quad (*)$$

Since B and B' both are normal orthogonal bases of K/F, by definition we get

$$tr_{K/F}(\alpha^{q^i} \cdot \alpha^{q^j}) = tr_{K/F}(\beta^{q^i} \cdot \beta^{q^j}) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise,} \end{cases}$$

so that by $(*)$ we have $I = A \cdot I \cdot A^T = A \cdot A^T$. $\square$

We have proved that the transformation matrix between two normal orthogonal bases of K/F is orthogonal circulant. Conversely, given an arbitary orthogonal circulant matrix $A = [a_{i-j}]$ with entries in F, by multiplying a given normal orthogonal basis, in the form of a vector $B = (\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}})$ of $(K/F)^n$, with A (i.e. finding $B \cdot A$), we obtain a normal basis in the form as a vector $B' = (b_1, b_2, ..., b_n)$ of $(K/F)^n$ where $b_i = \sum_{k=0}^{n-1} \alpha^{q^k} a_{k-i}$ (since A is circulant invertible and B is a normal basis). In fact B' is a normal orthogonal basis. To prove this observe that $B' \cdot (B')^T = (B \cdot A)(B \cdot A)^T = B(AA^T)B^T = I$. By Chapter 2 Theorem 2.27, for any given $n = [K : F]$ the number of $n \times n$ orthogonal circulant matrices with entries in F is $\left|O_{(n,q)}\right|$. Therefore we have

THEOREM 4.6. *Let K be a Galois extension of degree n of the finite field $F = GF(q)$. If K/F has a normal orthogonal bases then it has exactly $\left|O_{(n,q)}\right|$ different normal orthogonal bases (that is, $\left|O_{(n,q)}\right|/n$ different normal orthogonal bases up to cyclic permutations).*

Example. Let $F = GF(2)$, let K be an extension of F with minimal polynomial $x^3 + x^2 + 1$ in $F[x]$. Then K is a *Galois* extension of F with the degree 3. By

Theorem 4.3, K/F has at least one normal basis. Let α be a root of $x^3 + x^2 + 1$. For $\alpha_1 = \alpha$, $\alpha_2 = \alpha^2$, and $\alpha_3 = \alpha^4 = \alpha^2 + \alpha + 1$, it is easy to see that α_1, α_2, α_3 is a basis of K/F. By definition it is a normal basis. Since $tr(\alpha) = \alpha + \alpha^2 + \alpha^4 = 1$, by Lemma 4.2 we have

$$tr_{K/F}(\alpha_1^2) = tr_{K/F}(\alpha_2^2) = tr_{K/F}(\alpha_3^2) = 1.$$

Also

$$tr_{K/F}(\alpha_1\alpha_2) = tr_{K/F}(\alpha_1\alpha_3) = tr_{K/F}(\alpha_2\alpha_3) = 0.$$

So that α_1, α_2, α_3 is a normal orthogonal basis of K/F. Since $[K : F] = 3$, by Theorem 4.6 K/F has exactly $|O_{(3,2)}| = 3$ different normal orthogonal bases. Now let us use the method given in Chapter 3 (or you can use the program in Chapter 5) to construct the orthogonal group $\mathcal{O}$ of $F[x]/(x^3 + 1)$. Since

$$\frac{F[x]}{(x^3+1)} \cong \frac{F[x]}{(x+1)} \times \frac{F[x]}{(x^2+x+1)}$$

we have

$$\mathcal{O} \cong \mathcal{O}' \times \mathcal{O}''$$

where $\mathcal{O}$, $\mathcal{O}'$ and $\mathcal{O}''$ are the orthogonal groups of $F[x]/(x^3 + 1)$, $F[x]/(x + 1)$ and $F[x]/(x^2 + x + 1)$ respectively. We have $\mathcal{O}' = \{1\}$, $\mathcal{O}'' = \{1, x, x + 1\}$. Let e_1 and e_2 denote the local idempotents of $\mathcal{O}'$ and $\mathcal{O}''$. Since $1 = x(x + 1) + (x^2 + x + 1)$ and $[x(x + 1)]^2 = x(x + 1)$, $(x^2 + x + 1)^2 = (x^2 + x + 1) \bmod x^3 + 1$ over F, then we have

$$e_1 = x^2 + x + 1$$

$$e_2 = x(x+1).$$

Therefore the first rows for the three elements of $\mathcal{O}$ are $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$. The corresponding three orthogonal circulants are

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

By multiplying A_1, A_2 and A_3 with the normal orthogonal basis $(\alpha_1, \alpha_2, \alpha_3)$, we obtain three different normal orthogonal bases $B_1 = \{\alpha_1, \alpha_2, \alpha_3\}$, $B_2 = \{\alpha_3, \alpha_1, \alpha_2\}$ and $B_3 = \{\alpha_2, \alpha_3, \alpha_1\}$.

Chapter 5. The Program for Constructing the Orthogonal Group of $F[x]/(x^n - 1)$.

Let p be a prime number, n positive integers, let $F_p = \mathbb{Z}/p\mathbb{Z}$ (the field of fractio of $\mathbb{Z}/p\mathbb{Z}$) and let $F = GF(q)$ be the *Galios* extension of F_p where $q = p^k$. For a given positive integer N, let $P = x^N - 1$. In this chapter we give an introduction f the program which can be used to construct the orthogonal group for the polynomi ring $F[x]/(P)$. We separate the program into two steps: (I) Construct the fini field $F = GF(q)$. (II) Construct the orthogonal group of $F[x]/(P)$.

(I) Since $F = GF(q)$ is a extension of F_p with degree k, for any fixed p and k v can find a monic irreducible polynomial with degree k, saying g_0, over F_p. Let α a root of g_0 then g_0 is the minimal polynomial of α over F_p and the multiplicati group $[F = GF(q)]^\times$ can be generated by α. Therefore each element of $F = GF($ can be written in the form of α with $g_0(\alpha) = 0$.

(II) This step is more complicated, first we factor polynomial P over $F = GF(q$ let g be an arbitrary irreducible factor of P then g is one of the following fo different forms.

(1) $x - 1$.

(2) $x + 1$.

(3) the factor of P is irreducible reciprocal over $F = GF(q)$ which has eve degree.

(4) the factor of P is irreducible nonreciprocal over $F = GF(q)$ but there exis unique one factor g' of P, g' has the same degree as g and $g \cdot g'$ is an irreducib reciprocal polynomial.

In order to read the program easily, the all variables used in the program should be exactly the same as we used in this chapter. Here we give a notation for some important variables.

n_0: if $p = 2$ we define $n_0 = 0$ otherwise $n_0 = 1$.

n_1: if $x + 1$ is a factor of P then $n_1 = 1$ otherwise $n_1 = 0$.

n_2: denote the numbers of irreducible reciprocal factors of P over $GF(q)$ (they have even degree).

n_3: denote the numbers of irreducible nonreciprocal factors of P over $GF(q)$.

$m.1$: denote the numbers of the irreducible factors of P over $GF(q)$.

m: denote the multiplicity of the irreducible factors of P over $GF(q)$ where $m = p^l$ for some positive integer l.

Let $P = g_1^{r_1} \cdot g_2^{r_2} \cdots g_{m.1}^{r_{m.1}}$ be the irreducible factor decomposition of P, then we have $r_1 = r_2 = \cdots = r_{m.1} = m$ for some positive integer m. If $p \neq 2$ and $x + 1$ is a factor of P, we assume that $g_1 = x+1$ and $g_2 = x-1$, it may happen that $x+1$ is not a factor of P, then we assume that $g_1 = x - 1$. If $p = 2$, we assume that $g_1 = x + 1$. For $3 \leq i \leq n_2 + 2$ (or $2 \leq i \leq n_2 + 1$ depends whether or not $x + 1$ is a factor of P), let g_i denote the irreducible reciprocal factors of P over $GF(q)$ (they have even degree). For $n_2 + 2 \leq i \leq m.1$ (or $n_2 + 1 \leq i \leq m.1$), let g_i denote the irreducible nonreciprocal factors of P over $GF(q)$. Suppose that $E = \{e.i : 1 \leq i \leq m.1\}$ where $e.i$ are the idempotents of g_i^m. Let $e.i = h_i(x) \times (P/g_i^m)$, then $e.i$ is congruent to 1 mod g_i^m. We can obtain $e.i$ (i.e. find h_i) by using Euclid's algorithm.

Constructing the orthogonal groups of $F[x]/((x + 1)^m)$ and $F[x]/((x + 1)^m)$.

If $p \neq 2$ ($n_0 = 1$).

(1)Constructing the orthogonal group O_m of $F[x]/((x+1)^m)$ (if $n_1 = 1$).

Suppose that $f = f_0 + f_1(x+1) + ... + f_{m-1}(x+1)^{m-1}$ is an element of orthogonal group of $F[x]/((x+1)^m)$, we have to determinate all f_i for $0 \leq i \leq m-1$. It is easy to see $f_0 \in \{1, p-1\}$. For i odd, $f_i \in F$. For i even, let $f = f_0 + f_1(x+1) + .. + f_{i-1}(x+1)^{i-1}$ belongs to O_i, i.e. the orthogonal group of $F[x]/((x+1)^i)$, let $f' = f(x^{-1})$ in $F[x]/((x+1)^m)$. Calculating $f \cdot f' - 1$, we write $f \cdot f' - 1$ in the form of $(x+1)$'s powers. Taking the coefficient of $(x+1)^i$ and denote it by d then $f_i = -f_0 \frac{d}{2}$ so that we have $f = f_0 + f_1(x+1) + ... + f_i(x+1)^i$ belongs to O_{i+1}. Now we already discuss all cases for f_i, by repeating the processing for i from 0 to $m-1$ (for every different combination of f_i), we can obtain all elements in O_m.

(2)Constructing the orthogonal group O_m of $F[x]/((x-1)^m)$.

This is almost the same processing as (1), here y is the inverse element of x in $F[x]/((x-1)^m)$ and we change all $x+1$ in (1) to $x-1$.

If $p = 2$ ($n_0 = 0$).

Constructing the orthogonal group O_m of $F[x]/((x+1)^m)$.

Suppose that $f = f_0 + f_1(x+1) + ... + f_{m-1}(x+1)^{m-1}$ is an element of orthogonal group $F[x]/(x+1)^m$, then we have to determinate all f_i for $0 \leq i \leq m-1$. It is obvious $f_0 = 1$. Since $m = p^l$, we have $m = 2^l$ for some positive integer l so that $m-1$ is always odd. If $m-1 = 1$, then $f_1 \in F$. If $m-1 > 1$, then $f_1 \in \{0, 1\}$. For i even (so $i < m-1$), $f_i \in F$, let $f = f_0 + f_1(x+1) + .. + f_i(x+1)^i$ belongs to O_{i+1}, i.e. the orthogonal group of $F[x]/((x+1)^{i+1})$. Now incrementing i by 1, if $i+1 = m-1$ then $f_{i+1} = f_{m-1}$ belongs to F, else if $i+1 < m-1$, let $f' = f(x^{-1})$ in $F[x]/((x+1)^m)$. Calculating $f \cdot f' - 1$, we write $f \cdot f' - 1$ in the form of $(x+1)$'s

powers. Taking the coefficient of $(x+1)^{i+2}$ and denote it by d then $f_{i+1} = d$ so we have that $f = f_0 + f_1(x+1) + ... + f_{i+1}(x+1)^{i+1}$ belongs to O_{i+1}. Until now, we already discuss all cases for f_i, repeating the processing for i from 0 to $m-1$ (for every different combination of f_i), we can get all elements in O_m.

Constructing the orthogonal groups O_m of $F[x]/(g^m)$ where g is an irreducible reciprocal factor of P.

If $n_2 \neq 0$ (if some irreducible factors of P are reciprocal).

Let g be an irreducible reciprocal factor of P. Suppose that $f = f_0 + f_1 G + ... + f_{m-1} G^{m-1}$ is an element of orthogonal group O_m of $F[x]/(g^m)$. Then $f_0 \in O_1$, the orthogonal group of $F[x]/(g)$ which has order $q^s + 1$ where $2s$ is the degree of g. To find the group O_1, let $r(x) \in F[x]/(g)$, if $r(x) \cdot r(x^{-1}) = 1$ in $F[x]/(g)$ then $r \in O_1$. Let $f = f_0 + f_1 g + .. + f_i g^i$ be an element of O_{i+1}, let d denote the degree of g. Calculating $f(x) * f(x^{-1}) - 1$ and write it in the form of g's powers. Taking the coefficient of g^{i+1} and denote it by D then $f_{i+1} = f_0 \cdot (S * D + (y.1^{(}d/2))^i \cdot F_1)$ so that we have $f = f_0 + f_1 g + ... + f_{i+1} g^{i+1}$ belongs to O_{i+1} (F_1 is the fixed field of F under the substituting $x = x^{-1}$ for each element of F). If $p \neq 2$, $S = (p-1)/2$. If $p = 2$, $S = x/(x + x^{-1})$. Repeating the processing for i from 0 to $m-1$ (for every different combination of f_i), we can get all elements in O_m.

Constructing the orthogonal groups $O_{(i,j)}$ of $F[x]/(g_i^m) \times F[x]/(g_j^m)$ where g_i, g_j are irreducible nonreciprocal factors of P and $g_i \cdot g_j$ is reciprocal.

If $n_3 \neq 0$ (if some irreducible factors of P are nonreciprocal).

Let g_i and g_j be a pair of irreducible nonreciprocal factors of P, i.e $g_i \cdot g_j$ is reciprocal. Let x denote the root of g_i, let $F_i^{\times}$ and $F_j^{\times}$ denote the groups of units

of $F[x]/(g_i^m)$ and $F[x]/(g_j^m)$ respectively, then $F_i^\times = \{f_0 + f_1 g_i + \cdots + f_{m-1} g_i^{m-1} : f_0 \in (F[x]/(g_i))^\times, f_k \in F[x]/(g_i)\}$. For each element $r(x) \in F_i^\times$, let $r'(x) = r(x^{-1})$ in $F_j^\times$ then we can find the inverse element of $r'(x)$, saying $(r')^{-1}$, in $F_j^\times$. Therefore $(r, (r')^{-1})$ is an orthogonal pair of $(F[x]/(g_i^m) \times (F[x]/(g_j^m)$. Repeating the processing above for all elements of $F_i^\times$, we can find all pairs of $O_{(i,j)}$.

Finally, let O denote orthogonal group of $F[x]/(x^N - 1)$, then $O = \{f : f = f.1 \cdot e.1 + f.2 \cdot e.2 + ... + f.(m.1) \cdot e.(m.1)\}$ where $f.i$ $(1 \leq i \leq m.1)$ is an arbitrary orthogonal element in $F[x]/(g_i^m)$ (for some i, j, $(f.i, f.j)$ may be a orthogonal pair of $(F[x]/(g_i^m) \times (F[x]/(g_j^m)$.

References

1. Julio R. Bastida, *Field Extensions and Galois Theory*, Addison-Wesley, California. (1984).
2. S. Lang, *Algebra*, Addison-Wesley, California. (1984).
3. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Mass. (1969).
4. F. J. MacWilliams, *Orthogonal circulant matrices over finite fields and how to find them*, J. Combinatiorial Theorv. **10** (1971). 1–17.
5. David S. Dummit and Richard M. Foote, *Abstract Algebra*, Prentice-Hall. New Jersey 07632. (1991).
6. Harold M. Edwards, *Galois Theory*, Springer-Verlag, New York, Berlin, Heidelberg and Tokyo..
7. Dieter Jungnickel, Thomas Beth and Willi Geiselmann, *A note on orthogonal circulant matrices over finite fields*, Arch. Math. **62** (1994), 126–133.
8. K.A.Byrd and T.P.Vaughan, *Counting and Constructing orthogonal Circulants*, Combinatorial Theory, Series A 24, **62** (1978), 34–49.
9. Bernard R. McDonald, *Finite Rings with Identity*. Marcel Dekker. New York..
10. Pierre Samuel, *Algebraic Theory of Numbers*, Hermann Publishers in Arts and Sciences, Paris, France (1970).
11. Fred Abraham Lempel and Marcelo J. Weinberger, *Self-Complementary Normal Bases in Finite Fields*, Siam J. Disc. Math. **1, No. 2** (May 1988), 193–198.
12. R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, California. (1983).
13. Andre Heck, *Introduction to Maple*, Springer-Verlag, New York. (1993).

APPENDIX

```
> # The first program which can be used to construct an
> # orthogonal group of nxn circulant matrix
> with(linalg):
> restart:
> #Giving the following values for three parameters of p,
  k, and N before the line of signs "###...".
> p:=2; #Give p.
> k:=2: #Let F=GF(p^k), give k.
> N:=6: #Give the degree of x^N-1.
> ##########################################################
> P:=x^N-1 mod p;
> #the following program codes (before "###...") are used
  to factor the polynomial x^N-1=g[0]*g[1]*...*g[r] over
  GF(q) for some r. where g[i] either is reciprocal
  polynomial or g[i] is not a reciprocal but g[i]*g[i+1]
  (or g[i]*g[i-1]) is a reciprocal.
> readlib(GF):
> F:=GF(p,k):
> d:=F[extension]:
> d:=F[ConvertOut](d):
> g[0]:=subs(`?`=x, d);
> d:='d':
> k='k':
> if degree(g[0])>1 then
> alias(alpha=RootOf(g[0],x)):
> fi:
> if degree(g[0])>1 then
> P:=Factor(P,alpha) mod p:
> fi:
> if degree(g[0])<=1 then
```

```
> P:=Factor(P) mod p:
> fi:
> P:=P;
> n[0]:=0:
> n[1]:=1:
> n[2]:=0:
> n[3]:=0:
> g[1]:=x-1 mod p:
> if whattype(P)<>`*` then
> m.1:=1:
> m:=degree(P):
> if p<>2 then
> n[0]:=1:
> n[1]:=0:
> fi:
> else
> readlib(recipoly):
> m.1:=nops(P):
> P.1:=P:
> for i from 1 to nops(P.1) do
> f(i):=subs(x=1,op(i,P.1)) mod p:
> if f(i)=0 then
> m:=degree(op(i,P.1)):
> break:
> fi:
> od:
> P.1:=Normal(P.1/g[1]^m) mod p:
> if whattype(P.1)=`*` then
> m.2:=nops(P.1):
> else
> m.2:=1:
```

```
> fi:
> if p<>2 then
> n[0]:=1:
> n[1]:=0:
> for i from 1 to m.2 do
> if m.2=1 then
> if m<>1 then
> f(i):=op(1,P.1):
> else
> f(i):=P.1:
> fi:
> else
> if m<>1 then
> f(i):=op(1,op(i,P.1)):
> else
> f(i):=op(i,P.1):
> fi:
> fi:
> f.1(i):=subs(x=-1,f(i)) mod p:
> if f.1(i)=0 then
> g[1]:=x+1 mod p:
> g[2]:=x-1 mod p:
> n[1]:=1:
> P.1:=Normal(P.1/g[1]^m) mod p:
> break:
> fi:
> od:
> fi:
> if whattype(P.1)=`*` then
> m.2:=nops(P.1):
> elif P.1<>1 then
```

```
> m.2:=1:
> fi:
> if P.1<>1 then
> if m.2+1=m.1 then
> V:=[ ]:
> for i from 1 to m.2 do
> if m.2=1 then
> if m<>1 then
> f(i):=op(1,P.1):
> else
> f(i):=P.1:
> fi:
> else
> if m<>1 then
> f(i):=op(1,op(i,P.1)):
> else
> f(i):=op(i,P.1):
> fi:
> fi:
> f.1(i):=recipoly(subs(alpha=2,f(i)),x):
> if f.1(i)=true then
> V:=V union [f(i)]:
> fi:
> od:
> n[2]:=nops(V):
> for i from 1 to nops(V) do
> P.1:=Normal(P.1/V[i]^m) mod p:
> g[i+1]:=V[i] mod p:
> od:
> if nops(V)+1<>m.1 then
> M:=[ ]:
```

```
> for i from 1 to nops(P.1) do
> if m<>1 then
> f(i):=op(1,op(i,P.1)):
> else
> f(i):=op(i,P.1):
> fi:
> M:=M union {f(i)}:
> od:
> for i from 1 to nops(M) do
> for j from 1 to nops(M) do
> f(i,j):=evala(Expand(M[i]*M[j])) mod p:
> f.1(i,j):=recipoly(subs(alpha=2,f(i,j)),x):
> if f.1(i,j)=true then
> g[nops(V)+2*i]:=M[i] mod p:
> g[nops(V)+2*i+1]:=M[j] mod p:
> break:
> fi:
> od:
> od:
> n[3]:=m.1-(nops(V)+n[2]+1):
> fi:
> elif m.2+2=m.1 then
> V:=[ ]:
> for i from 1 to m.2 do
> if m.2=1 then
> if m<>1 then
> f(i):=op(1,P.1):
> else
> f(i):=P.1:
> fi:
> else
```

```
> if m<>1 then
> f(i):=op(1,op(i,P.1)):
> else
> f(i):=op(i,P.1):
> fi:
> fi:
> f.1(i):=recipoly(subs(alpha=2,f(i)),x):
> if f.1(i)=true then
> V:=V union {f(i)}:
> fi:
> od:
> n[2]:=nops(V):
> for i from 1 to nops(V) do
> P.1:=Normal(P.1/V[i]^m) mod p:
> g[i+2]:=V[i] mod p:
> od:
> if nops(V)+2<>m.1 then
> M:={ }:
> for i from 1 to nops(P.1) do
> if m<>1 then
> f(i):=op(1,op(i,P.1)):
> else
> f(i):=op(i,P.1):
> fi:
> M:=M union {f(i)}:
> od:
> for i from 1 to nops(M) do
> for j from 1 to nops(M) do
> f(i,j):=evala(Expand(M[i]*M[j])) mod p:
> f.1(i,j):=recipoly(subs(alpha=2,f(i,j)),x):
> if f.1(i,j)=true then
```

```
> g[nops(V)+2*i]:=M[i] mod p:
> g[nops(V)+2*i+1]:=M[j] mod p:
> break:
> fi:
> od:
> od:
> n[3]:=m.1-(nops(V)+n[2]+2):
> fi:
> fi:
> fi:
> fi:
> ##########################################################
> #the following program codes (before "###...") are used
  to find all idempotents elements of F[x]/(x^N-1).
> E:=[seq(e.i, i=1..m.1)]:
> for i from 1 to m.1 do
> e.i:=sort(Expand(P/g[i]^m)) mod p:
> od:
> T:=[seq(degree(g[i]^m), i=1..m.1)]:
> for i from 1 to m.1 do
> v:=0:
> v.1:=0:
> f:=E[i] mod p:
> V:=evala(Expand(g[i]^m)) mod p:
> for j from 1 to T[i] do
> r:=Rem(f,V,x,'q[i,j]') mod p:
> q[i,j]:=q[i,j] mod p:
> if r=subs(x=1,r) then
> q.1:=q[i,j]:
> t[i,j]:=r-v:
> q[i,j]:=q.1-v.1:
```

```
> v:=r:
> v.1:=q.1:
> elif r<>subs(x=1,r) then
> f:=V:
> V:=r:
> t[i,j]:=r:
> fi:
> od:
> od:
> for i from 1 to m.1 do
> V.i:=[ ]:
> for j from 1 to T[i] do
> if t[i,j]<>0 then e[i,j]:=t[i,j]:
> V.i:=V.i union {e[i,j]}:
> fi:
> od:
> o.i:=nops(V.i):
> od:
> for i from 1 to m.1 do
> for j from 1 to o.i do
> u[i,j]:=u[i,j-2]-q[i,j]*u[i,j-1]:
> od:
> od:
> for i from 1 to m.1 do
> e[i]:=evala(Expand(subs(u[i,0]=0,u[i,o.i]/t[i,o.i])))
  mod p:
> od:
> for i from 1 to m.1 do
> if degree(g[0])>1 then
> e[i]:=Factor(subs(u[i,-1]=E[i], e[i]),alpha) mod p:
> else
```

```
> e[i]:=Factor(subs(u[i,-1]=E[i], e[i])) mod p:
> fi:
> od:
> E:=[seq(e[i],i=1..m.1)] mod p:
> ############################################################
> #the following program codes (before "###...") are used
  to construct the field GF(q).
> readlib(GF):
> F:=GF(p,degree(g[0]),g[0]):
> beta:=F[PrimitiveElement]():
> for i from 1 to p^(degree(g[0]))-1 do
> b.i:=F[`^`](beta,i):
> b.i:=F[ConvertOut](b.i):
> od:
> b.0:=0:
> F:=[seq(subs(x=alpha,b.i), i=0..p^(degree(g[0]))-1)]:
> ############################################################
> #the following program codes (before "###...") are used
  to construct the orthogonal groups F[x]/(x+1)^m and
  F[x]/(x-1)^m.
> f:='f':
> if n[0]=1 then
> if n[1]=1 then
> if m=1 then
> U.1:=[1,p-1]:
> U.2:=U.1:
> else
> y:=-x^(m-1): # defining y, the inverse of x in
  F[x]/(g[1])^m mod p
> F.1:=[1,p-1]: # defining O[1]
```

```
> z:= { w.1 =g[1]}:
> z.1:={w=w.1^m}:
> l:=2:
> for j from 1 by 2 to m-1 do
> for i from 1 to l do
> for k from 1 to nops(F) do
> f(i,k):=F.l[i]+F[k]*g[l]^j mod p:
> f.l(i,k):=evala(Expand(subs(x=y, f(i,k)))) mod p:
> f.l(i,k):=evala(Expand(f(i,k)*f.l(i,k)-l)) mod p:
> f.l(i,k):=simplify(f.l(i,k),z, [x,w.l]) mod p:
> f.l(i,k):=simplify(f.l(i,k),z.l, [w.l,w]) mod p:
> f.l(i,k):=subs(w=0,f.l(i,k)) mod p:
> f.l(i,k):=evala(Expand(f.l(i,k))) mod p:
> f.l(i,k):=collect(f.l(i,k), w.l) mod p:
> d(i,k):=coeff(f.l(i,k), w.l^(j+l)) mod p:
> f.2(i,k):=simplify(f(i,k),z,[x,w.l]) mod p:
> f(i,k):= f(i,k)-subs(w.l=0,
  f.2(i,k))*d(i,k)/2*g[l]^(j+l) mod p:
> f(i,k):=evala(Expand(f(i,k))) mod p:
> f(i,k):=simplify(f(i,k),z, [x,w.l]) mod p:
> od:
> od:
> T:=[seq(seq(f(i,k), i=l..l), k=l..nops(F))] mod p:
> U.l:=[seq(seq(collect(f(i,k),w.l), i=l..l),
  k=l..nops(F))] mod p:
> T:=subs(w.l=x+l, T):
> q:=nops(U.l):
> F.l:=T mod p:
> l:=q:
> od:
> U.l: # all elements of O in F[x]/g[l]^m
```

```
> nops(U.1): # the order of 0 in F[x]/g[1]^m
> y:=x^(m-1): # defining y, the inverse of x in
  F[x]/(g[2])^m mod p
> F.1:=[1,p-1]: # defining 0[1]
> z:={w.2=g[2]}:
> z.1:={w=w.2^m}:
> l:=2:
> for j from 1 by 2 to m-1 do
> for i from 1 to l do
> for k from 1 to nops(F) do
> f(i,k):=F.1[i]+F[k]*g[2]^j mod p:
> f.1(i,k):=evala(Expand(subs(x=y, f(i,k)))) mod p:
> f.1(i,k):=evala(Expand(f(i,k)*f.1(i,k)-1)) mod p:
> f.1(i,k):=simplify(f.1(i,k),z, [x,w.2]) mod p:
> f.1(i,k):=simplify(f.1(i,k),z.1, [w.2,w]) mod p:
> f.1(i,k):=subs(w=0,f.1(i,k)) mod p:
> f.1(i,k):=evala(Expand(f.1(i,k))) mod p:
> f.1(i,k):=collect(f.1(i,k), w.2) mod p:
> d(i,k):=coeff(f.1(i,k), w.2^(j+1)) mod p:
> f.2(i,k):=simplify(f(i,k),z,[x,w.2]) mod p:
> f(i,k):= f(i,k)-subs(w.2=0,
  f.2(i,k))*d(i,k)/2*g[2]^(j+1) mod p:
> f(i,k):=evala(Expand(f(i,k))) mod p:
> f(i,k):=simplify(f(i,k),z, [x,w.2]) mod p:
> od:
> od:
> T:=[seq(seq(f(i,k), i=1..l), k=1..nops(F))] mod p:
> U.2:=[seq(seq(collect(f(i,k),w.2), i=1..l),
  k=1..nops(F))] mod p:
> T:=subs(w.2=x-1, T):
```

```
> q:=nops(U.2):
> F.1:=T mod p:
> l:=q:
> od:
> U.2: # all elements of O in F[x]/g^m
> nops(U.2): # the order of O in F[x]/g^m
> fi:
> else
> if m=1 then
> U.1:=[1,p-1]:
> else
> y:=x^(m-1): # defining y, the inverse of x in
  F[x]/(g[1])^m mod p
> F.1:=[1,p-1]: # defining O[1]
> z:={w.1 =g[1]}:
> z.1:={w=w.1^m}:
> l:=2:
> for j from 1 by 2 to m-1 do
> for i from 1 to l do
> for k from 1 to nops(F) do
> f(i,k):=F.1[i]+F[k]*g[1]^j mod p:
> f.1(i,k):=evala(Expand(subs(x=y, f(i,k)))) mod p:
> f.1(i,k):=evala(Expand(f(i,k)*f.1(i,k)-1)) mod p:
> f.1(i,k):=simplify(f.1(i,k),z, [x,w.1]) mod p:
> f.1(i,k):=simplify(f.1(i,k),z.1, [w.1,w]) mod p:
> f.1(i,k):=subs(w=0,f.1(i,k)) mod p:
> f.1(i,k):=evala(Expand(f.1(i,k))) mod p:
> f.1(i,k):=collect(f.1(i,k), w.1) mod p:
> d(i,k):=coeff(f.1(i,k), w.1^(j+1)) mod p:
> f.2(i,k):=simplify(f(i,k),z,[x,w.1]) mod p:
> f(i,k):= f(i,k)-subs(w.1=0,
```

```
  f.2(i,k))*d(i,k)/2*g[1]^(j+1) mod p:
> f(i,k):=evala(Expand(f(i,k))) mod p:
> f(i,k):=simplify(f(i,k),z, [x,w.1]) mod p:
> od:
> od:
> T:=[seq(seq(f(i,k), i=1..l), k=1..nops(F))] mod p:
> U.1:=[seq(seq(collect(f(i,k),w.1), i=1..l),
  k=1..nops(F))] mod p:
> T:=subs(w.1=x-1, T):
> q:=nops(U.1):
> F.1:=T mod p:
> l:=q:
> od:
> U.1: # all elements of 0 in F[x]/g[1]^m
> nops(U.1): # the order of 0 in F[x]/g[1]^m
> fi:
> fi:
> else
> if m=1 then
> U.1:=[1]:
> else
> y:=x^(m-1): # defining y, the inverse of x in
  F[x]/g[1]^m mod p
> F.0:=[0]:
> F.1:=[1]:
> z:=[w.1 =g[1]]:
> z.1:={w=w.1^m}:
> h.1:=1:
> h:=1:
> for j from 0 to m/2-1 do
> if 2*j+1=m-1 then
```

```
> for l from 1 to h.1 do
> for i from 1 to h do
> for k from 1 to nops(F) do
> f(l,i,k):=F.0[l]+F.1[i]*g[l]^(2*j)+F[k]*g[l]^(2*j+1) mod
  p:
> f(l,i,k):=simplify(f(l,i,k),z,[x,w.1]) mod p:
> f(l,i,k):=evala(Expand(f(l,i,k))) mod p:
> f(l,i,k):=collect(f(l,i,k),w.1) mod p:
> od:
> od:
> od:
> elif j=0 then
> for l from 1 to h.1 do
> for i from 1 to h do
> for k from 1 to nops(F) do
> f(l,i,k):=F.0[l]+F.1[i]*g[l]^(2*j)+F[k]*g[l]^(2*j+1) mod
  p:
> od:
> od:
> od:
> F.0:=[seq(seq(seq(f(l,i,k), l=1..h.l), i=1..h),
  k=1..nops(F))] mod p:
> h.l:=nops(F.0):
> F.1:=F mod p:
> h:=nops(F):
> else
> d:='d':
> for l from 1 to h.l do
> for i from 1 to nops(F) do
> f(l,i):=F.0[l]+F.1[i]*g[l]^(2*j) mod p:
```

```
> f.1(1,i):=evala(Expand(subs(x=y, f(1,i)))) mod p:
> f.1(1,i):=evala(Expand(f(1,i)*f.1(1,i)+1)) mod p:
> f.1(1,i):=simplify(f.1(1,i),z, [x,w.1]) mod p:
> f.1(1,i):=simplify(f.1(1,i),z.1, [w.1,w]) mod p:
> f.1(1,i):=subs(w=0,f.1(1,i)) mod p:
> f.1(1,i):=evala(Expand(f.1(1,i))) mod p:
> f.1(1,i):=collect(f.1(1,i), w.1) mod p:
> d(1,i):=coeff(f.1(1,i), w.1^(2*j+2)) mod p:
> f(1,i):= f(1,i)+d(1,i)*g[1]^(2*j+1) mod p:
> od:
> od:
> F.0:=[seq(seq(f(1,i), 1=1..h.1), i=1..nops(F))] mod p:
> h.1:=nops(F.0):
> fi:
> od:
> U.1:=[seq(seq(seq(f(1,i,k), 1=1..h.1), i=1..h),
  k=1..nops(F))] mod p:#all elements of O in F[x]/g[1]^m.
> nops(U.1): # the order of O in F[x]/g[1]^m
> fi:
> fi:
> ##################################################
> #the following program codes (before "###...") are used
  to construct the orthogonal groups F[x]/(g[i])^m where
  g[i]is different with x+1 or x-1 and g[i] is reciprocal
  polynomial.
> if n[2]<>0 then
> if m=1 then
> y:='y':
> for 1 from n[0]+n[1]+1 to n[0]+n[1]+n[2] do
> a[0]:=evala(subs(x=0,g[1])) mod p:
```

```
> d:=degree(g[1]):
> y.1:=x^(-1)*evala(g[1]-a[0]) mod p:
> y.1:=Normal(y.1) mod p:
> y.1:=evala(Expand(-a[0]^(-1)*y.1)) mod p:
> y:=x^(-1)*evala(g[1]-a[0]) mod p:
> y:=Normal(y) mod p:
> y:=evala(Expand(-(a[0])^(-1)*y)) mod p:
> F.1:=F:
> q.1:=nops(F):
> for i from 1 to d-1 do
> for j from 1 to nops(F) do
> for k from 1 to q.1 do
> f(j,k):=F.1[k]+F[j]*x^i mod p:
> od:
> od:
> V.0:=[seq(seq(f(j,k), j=1..nops(F)), k=1..q.1)] mod p:
> q.1:=nops(V.0):
> F.1:=V.0:
> od:
> V.1:=subs(x=y.1, V.0) mod p:
> W.1:=[ ]:
> z:=[w.1=g[1]]:
> z.1:=[w=w.1]:
> for i from 1 to q.1 do
> f(i):=evala(Expand(V.0[i]*V.1[i]-1)) mod p:
> f(i):=simplify(f(i),z,[x,w.1]) mod p:
> f(i):=subs(w.1=0,f(i)) mod p:
> f(i):=evala(Expand(f(i))) mod p:
> if f(i)=0  then W.1:=W.1 union [V.0[i]] mod p:
> fi:
> od:
```

```
> q.2:=nops(W.1):
> W.1:=[seq(W.1[i], i=1..q.2)]: # the group O[1]
> U.1:=W.1 mod p:
> od:
> else
> y:='y':
> for l from n[0]+n[1]+1 to n[0]+n[1]+n[2] do
> a[0]:=evala(subs(x=0,g[l])) mod p:
> d:=degree(g[l]):
> y.1:=x^(-1)*evala(g[l]-a[0]) mod p:
> y.1:=Normal(y.1) mod p:
> y.1:=evala(Expand(-a[0]^(-1)*y.1)) mod p: # defining y1,
  the inverse of x in F[x]/g[l] mod p:
> y:=x^(-1)*evala(g[l]^m-a[0]^m) mod p:
> y:=Normal(y) mod p:
> y:=evala(Expand(-(a[0]^m)^(-1)*y)) mod p: # defining y,
  the inverse of x in F[x]/g[l]^m mod p:
> F.1:=F:
> q.1:=nops(F):
> for i from 1 to d-1 do
> for j from 1 to nops(F) do
> for k from 1 to q.1 do
> f(j,k):=F.1[k]+F[j]*x^i mod p:
> od:
> od:
> V.0:=[seq(seq(f(j,k), j=1..nops(F)), k=1..q.1)] mod p:
> q.1:=nops(V.0):
> F.1:=V.0:
> od:
> V.1:=subs(x=y.1, V.0) mod p:
> W.1:=[ ]:
```

```
> z:={w.1=g[1]}:
> z.1:=[w=w.1^m]:
> if n[0]=0 then
> for i from 1 to q.1 do
> f(i):=simplify(V.1[i],z,[x,w.1]) mod p:
> f(i):=subs(w.1=0,f(i)) mod p:
> s:=evala(Expand(f(i)+V.0[i]+1)) mod p:
> if s=0 then
> S:=V.0[i] mod p:
> break:
> fi:
> od:
> else
> S:=(p-1)/2:
> fi:
> for i from 1 to q.1 do
> f(i):=evala(Expand(V.0[i]*V.1[i]-1)) mod p:
> f(i):=simplify(f(i),z,[x,w.1]) mod p:
> f(i):=subs(w.1=0,f(i)) mod p:
> f(i):=evala(Expand(f(i))) mod p:
> if f(i)=0  then W.1:=W.1 union {V.0[i]} mod p:
> fi:
> od:
> q.2:=nops(W.1):
> W.1:=[seq(W.1[i], i=1..q.2)]: # the group O[1]
> W.2:={ }:
> for i from 1 to q.1 do
> f(i):=simplify(V.1[i],z,[x,w.1]) mod p:
> f(i):=subs(w.1=0,f(i)) mod p:
> f(i):=evala(Expand(f(i))) mod p:
> if f(i)=V.0[i] then W.2:=W.2 union {V.0[i]} mod p:
```

```
> fi:
> od:
> q.3:=nops(W.2): #the order of F[1] is equal to p^(d/2)
> W.2:=[seq(W.2[i], i=1..q.3)]: # F[1], the fixed field of
  \tau in F[x]/g[1]
> W.3:=W.1:
> q.4:=q.2:
> for j from 1 to m-1 do
> for i from 1 to q.4 do
> f(i):=W.3[i] mod p:
> f.1(i):=subs(x=y, f(i)):
> f.1(i):=evala(Expand(f.1(i))) mod p:
> f.1(i):=evala(Expand(f(i)*f.1(i)-1)) mod p:
> f.1(i):=simplify(f.1(i),z, [x,w.1]) mod p:
> f.1(i):=simplify(f.1(i),z.1,[w.1,w]) mod p:
> f.1(i):=collect(f.1(i), w) mod p:
> f.1(i):=subs(w=0,f.1(i)) mod p:
> f.1(i):=evala(Expand(f.1(i))) mod p:
> D(i):=coeff(f.1(i), w.1^j) mod p:
> for k from 1 to q.3 do
> f(i,k):=f(i)+W.1[i]*(S*D(i)+(y.1^(d/2))^j*W.2[k])*g[1]^j
  mod p:
> f(i,k):= evala(Expand(f(i,k))) mod p:
> f(i,k):=simplify(f(i,k),z, [x,w.1]) mod p:
> f(i,k):=simplify(f(i,k),z.1, [w.1,w]) mod p:
> f(i,k):=subs(w=0, f(i,k)) mod p:
> f.1(i,k):=subs(w.1=0, f(i,k)) mod p:
> f.1(i,k):=evala(Expand(f.1(i,k))) mod p:
> f.2(i,k):=evala(Expand(f(i,k))) mod p:
> f.2(i,k):=collect(f.2(i,k),w.1) mod p:
> f(i,k):=subs(z,f(i,k)) mod p:
```

```
> f(i,k):=evala(Expand(f(i,k))) mod p:
> od:
> od:
> W.1:=[seq(seq(f.1(i,k), i=1..q.4), k=1..q.3)] mod p:
> W.3:=[seq(seq(f(i,k), i=1..q.4), k=1..q.3)] mod p:
> U.1:=[seq(seq(f.2(i,k), i=1..q.4), k=1..q.3)] mod p:
> q.4:=nops(W.3):
> od:
> od:
> fi:
> fi:
> ##########################################################
> #the following program codes (before "###...") are used
  to construct the orthogonal groups F[x]/(g[i])^m
  *F[x]/(g[j])^m where g[i] and g[j] are not reciprocal
  but g[i]*g[j] is a reciprocal.
> if n[3]<>0 then
> if m=1 then
> y:='y':
> for l from n[0]+n[1]+n[2]+1 by 2 to n[0]+n[1]+n[2]+n[3]
  do
> d:=degree(g[l]):#g[l] is any factor of a 2-cycle pair.
> a[0]:=evala(subs(x=0,g[l+1])) mod p:
> y[l]:=x^(-1)*evala(g[l+1]-a[0]) mod p:
> y[l]:=Normal(y[l]) mod p:
> y[l]:=evala(Expand(-a[0]^(-1)*y[l])) mod p: # defining
  y[l], the inverse of x in F[x]/(g[l+1])^m mod p:
> F.1:=F:
> q:=nops(F):
> if d>1 then
```

```
> for i from 1 to d-1 do
> for j from 1 to nops(F) do
> for k from 1 to q do
> f(j,k):=F.1[k]+F[j]*x^i mod p:
> od:
> od:
> U:=[seq(seq(f(j,k), j=1..nops(F)), k=1..q)] mod p:
> q:=nops(U):
> F.1:=U:
> od:
> else
> U:=F:
> q:=nops(U):
> fi:
> V:={ }:
> for i from 1 to q do
> if U[i]<>0 then V:=V union {U[i]} mod p:
> fi:
> od:
> U.1:=[seq(V[i], i=1..q-1)] mod p: #the multiplicative
  group of U
> z:={w=g[1+1]}:
> z.1:={w.1=g[1+1]}:
> for i from 1 to nops(U.1) do
> t.i:=evala(Expand(subs(x=y[1], U.1[i]))) mod p:
> t.i:=simplify(t.i,z,[x,w]) mod p:
> t.i:=simplify(t.i,z.1,[w,w.1]) mod p:
> t.i:=subs(w.1=0, t.i) mod p:
> t.i:=evala(Expand(t.i)) mod p:
> t.i:=collect(t.i, w.1) mod p:
> t.i:=subs(z, t.i) mod p:
```

```
> od:
> U:=[seq(t.i, i=1..q.1)] mod p:
> V:=convert(U,`set`):
> for i from 1 to nops(U) do
> for j from 1 to nops(V) do
> f(i,j):=evala(Expand(U[i]*V[j])) mod p:
> f(i,j):=simplify(f(i,j),z,[x,w]) mod p:
> f(i,j):=simplify(f(i,j),z.1,[w,w.1]) mod p:
> f(i,j):=subs(w.1=0, f(i,j)) mod p:
> f(i,j):=evala(Expand(f(i,j))) mod p:
> if f(i,j)=1 then k.i:=V[j] mod p:
> V:=V minus [V[j]]:
> break:
> fi:
> od:
> od:
> U.(1+1):=[seq(k.i, i=1..nops(U.1))] mod p:
> od:
> else
> y:='y':
> for l from n[0]+n[1]+n[2]+1 by 2 to n[0]+n[1]+n[2]+n[3]
  do
> d:=degree(g[l]):#g[l] is any factor of a 2-cycle pair.
> a[0]:=evala(subs(x=0,g[1+1]^m)) mod p:
> y[l]:=x^(-1)*evala(g[1+1]^m-a[0]) mod p:
> y[l]:=Normal(y[l]) mod p:
> y[l]:=evala(Expand(-a[0]^(-1)*y[l])) mod p: # defining
  y[l], the inverse of x in F[x]/(g[1+1])^m mod p:
> F.l:=F:
> q:=nops(F):
> if d>1 then
```

```
> for i from 1 to d-1 do
> for j from 1 to nops(F) do
> for k from 1 to q do
> f(j,k):=F.1[k]+F[j]*x^i mod p:
> od:
> od:
> U:=[seq(seq(f(j,k), j=1..nops(F)), k=1..q)] mod p:
> q:=nops(U):
> F.1:=U:
> od:
> else
> U:=F:
> q:=nops(U):
> fi:
> V:={ }:
> for i from 1 to q do
> if U[i]<>0 then V:=V union {U[i]} mod p:
> fi:
> od:
> V:=[seq(V[i], i=1..q-1)] mod p: #the multiplicative
  group of U
> F.1:=V:
> z.1:={w.1=g[1]}:
> z.2:={w=w.1^m}:
> q.1:=nops(V):
> for i from 1 to m-1 do
> for j from 1 to q do
> for k from 1 to q.1 do
> f(j,k):=F.1[k]+U[j]*g[1]^i mod p:
> f.1(j,k):=simplify(f(j,k),z.1,[x,w.1]) mod p:
> f.1(j,k):=simplify(f.1(j,k),z.2,[w.1,w]) mod p:
```

```
> f.1(j,k):=subs(w=0,f.1(j,k)) mod p:
> f.1(j,k):=evala(Expand(f.1(j,k))) mod p:
> f.1(j,k):=collect(f.1(j,k), w.1) mod p:
> f(j,k):=subs(z.1, f.1(j,k)) mod p:
> od:
> od:
> V.1:=[seq(seq(f(j,k), j=1..q), k=1..q.1)] mod p:
> U.1:=[seq(seq(f.1(j,k), j=1..q), k=1..q.1)] mod p:
> q.1:=nops(V.1):
> F.1:=V.1:
> od:
> z.3:={w.(1+1)=g[1+1]}:
> z.4:={w.4=w.(1+1)^m}:
> V.3:=V.1 mod p:
> for i from 1 to q.1 do
> t.i:=evala(Expand(subs(x=y[1], V.3[i]))) mod p:
> t.i:=simplify(t.i,z.3,[x,w.(1+1)]) mod p:
> t.i:=simplify(t.i,z.4,[w.(1+1),w.4]) mod p:
> t.i:=subs(w.4=0, t.i) mod p:
> t.i:=evala(Expand(t.i)) mod p:
> t.i:=collect(t.i, w.(1+1)) mod p:
> t.i:=subs(z.3, t.i) mod p:
> od:
> U:=[seq(t.i, i=1..q.1)] mod p:
> V:=convert(U,`set`):
> for i from 1 to nops(U) do
> for j from 1 to nops(V) do
> f(i,j):=evala(Expand(U[i]*V[j])) mod p:
> f(i,j):=simplify(f(i,j),z.3,[x,w.(1+1)]) mod p:
> f(i,j):=simplify(f(i,j),z.4,[w.(1+1),w.4]) mod p:
> f(i,j):=subs(w.4=0, f(i,j)) mod p:
```

```
> f(i,j):=evala(Expand(f(i,j))) mod p:
> if f(i,j)=1 then k.i:=V[j] mod p:
> V:=V minus {V[j]}:
> break:
> fi:
> od:
> k.i:=simplify(k.i,z.3,[x,w.(l+1)]) mod p:
> k.i:=evala(Expand(k.i)) mod p:
> k.i:=collect(k.i,w.(l+1)) mod p:
> od:
> U.(l+1):=[seq(k.i, i=1..q.1)] mod p:
> od:
> fi:
> fi:
> ##################################################
> #the following program codes (before "###...") are used
  to construct the elements of the orthogonal group of
  F[x]/(x^N-1).
> z:=[w=x^N-1] mod p:
> if m>1 then
> for i from 1 to m.1 do
> U.i:=subs(w.i=g[i],U.i) mod p:
> for j from 1 to nops(U.i) do
> U.i[j]:=sort(Expand(e[i]*U.i[j])) mod p:
> if degree(U.i[j])>=N then
> U.i[j]:=simplify(U.i[j],z,[x,w]) mod p:
> U.i[j]:=subs(w=0,U.i[j]) mod p:
> U.i[j]:=evala(Expand(U.i[j])) mod p:
> fi:
> od:
> od:
```

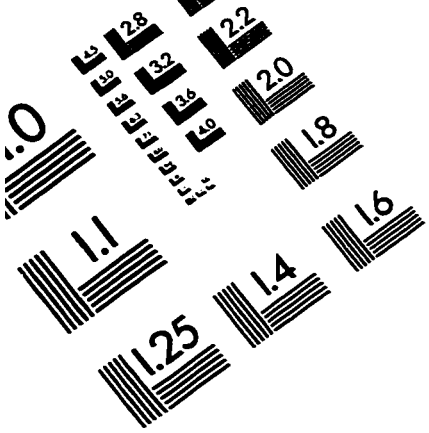
```
> else
> for i from 1 to m.1 do
> for j from 1 to nops(U.i) do
> U.i[j]:=sort(Expand(e[i]*U.i[j])) mod p:
> if degree(U.i[j])>=N then
> U.i[j]:=simplify(U.i[j],z,[x,w]) mod p:
> U.i[j]:=subs(w=0,U.i[j]) mod p:
> U.i[j]:=evala(Expand(U.i[j])) mod p:
> fi:
> od:
> od:
> fi:
> r:='r':
> n.2:=1:
> n.3:=1:
> if n[3]<>0 then #if some factor g[i] of x^N-1 is not
  reciprocal
> V:='V':
> L:=[ ]:
> for i from n[0]+n[1]+n[2]+1 by 2 to m.1 do
> for j from 1 to nops(U.i) do
> r(i,j):=evala(Expand(U.i[j]+U.(i+1)[j])) mod p:
> od:
> V(i,i+1):=[seq(r(i,j),j=1..nops(U.i))] mod p:
> L:=L union {V(i,i+1)} mod p:
> od:
> for i from (n[0]+n[1]+n[2])+1 by 2 to m.1 do
> n.3:=n.3*nops(U.i):
> od:
> fi:
> if n[2]<>0 then #if some factor g[i] of x^N-1 reciprocal
```

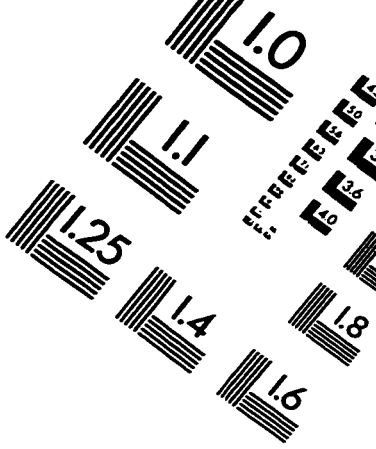
```
  and g[i] is different with x+1 or x-1.
> for i from n[0]+n[1]+1 to n[0]+n[1]+n[2] do
> n.2:=n.2*nops(U.i):
> od:
> fi:
> if n[0]=0 then
> M:=nops(U.1)*n.2*n.3:
> else
> M:=nops(U.1)*nops(U.2)*n.2*n.3:
> fi:
> if n[3]<>0 then
> b:=1:
> for i from n[0]+n[1]+n[2]+1 to n[0]+n[1]+n[2]+(n[3]/2)
  do
> for j from b to nops(L) do
> if L[j]<>0 then
> U.i:=L[j] mod p:
> b:=b+1:
> break:
> fi:
> od:
> od:
> fi:
> C:=n[0]+n[1]+n[2]+(n[3]/2):
> for i from 1 to C do
> n.i:=nops(U.i):
> od:
> V:='V':
> v:='v':
> if C<>1 then
> for k from 1 to C-1 do
```

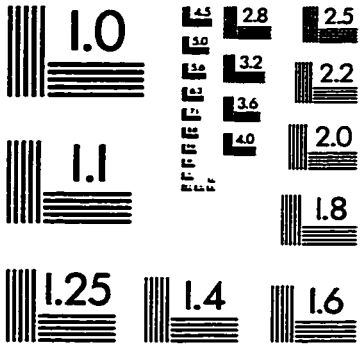
```
> for i.k from 1 to n.k do
> for i.(k+1) from 1 to n.(k+1) do
> v(i.k,i.(k+1)):=evala(Expand(U.k[i.k]+U.(k+1)[i.(k+1)]))
  mod p:
> od:
> od:
> V:=[seq(seq(v(i,j),i=1..n.k),j=1..n.(k+1))] mod p:
> U.(k+1):=V mod p:
> n.(k+1):=nops(V):
> od:
> h:='h':
> for i from 1 to M do
> for j from 1 to N-1 do
> h(i,0):=subs(x=0,V[i]) mod p:
> h(i,j):=coeff(V[i],x^j) mod p:
> od:
> H.i:=[seq(h(i,j),j=0..N-1)] mod p:
> od:
> else
> if N=1 then
> if n[0]<>0 then
> H.1:=1:
> H.2:=p-1:
> else
> H.1:=1:
> fi:
> else
> h:='h':
> for i from 1 to M do
> for j from 1 to N-1 do
> h(i,0):=subs(x=0,U.1[i]) mod p:
```

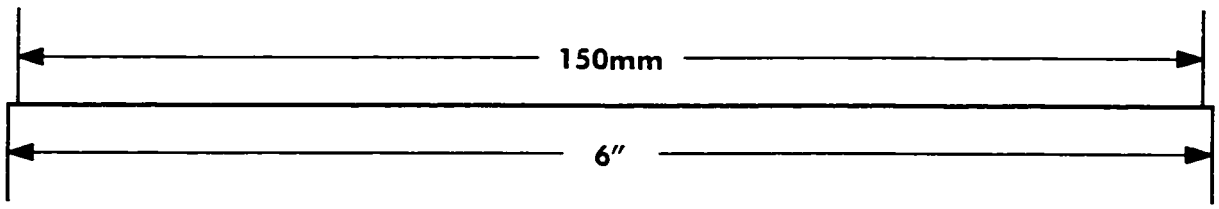
```
> h(i,j):=coeff(U.1[i],x^j) mod p:
> od:
> H.i:=[seq(h(i,j),j=0..N-1)] mod p:
> od:
> fi:
> fi:
> ##########################################################
> for i from 1 to M do #print all orthogonal elements of
  F[x]/(x^N-1).
> M.i=H.i;
> od;
>
> # The end of the first program
>
> # The second program can be used to check whether
> # a matrix above is an orthogonal or not. In this
  program we need the following values for four parameters
  p, N, g[0], and M before runing the program.
> with(linalg): with(numtheory):
> p:=2: #Given p
> N:=6: #Given N
> g[0]:=x^2+x+1: #Given the minimal polynomial g[0]
> alias(alpha=RootOf(g[0],x)):
> M:=vector([alpha,alpha,alpha,alpha,alpha,alpha+1]): #
  Given the first row of the matrix which you want to
  check.
> Id:=array(identity,1..N,1..N):
> T0:=delcols(Id,2..N):
> T1:=delcols(Id,1..1):
> T:=concat(T1,T0):
```

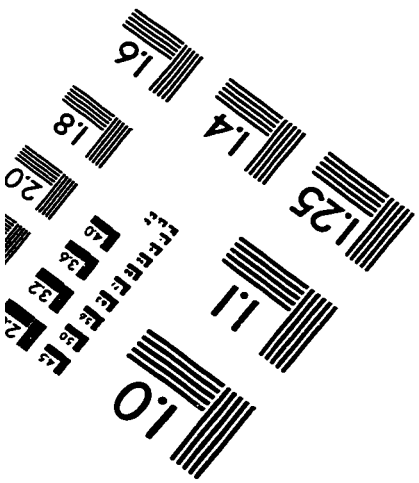
```
> A:=M[1]*Id+sum(M[i2]*T^(i2-1),i2=2..N):
> B:=evalm(A&*transpose(A)):
> C:=array(1..N,1..N):
> for j from 1 to N do:
> for k from 1 to N do:
> C[j,k]:=modp(evala(B[j,k]),p):
> od:
> od:
> evalm(B):
> evalm(C);
>
> # The end of the second program
>
```

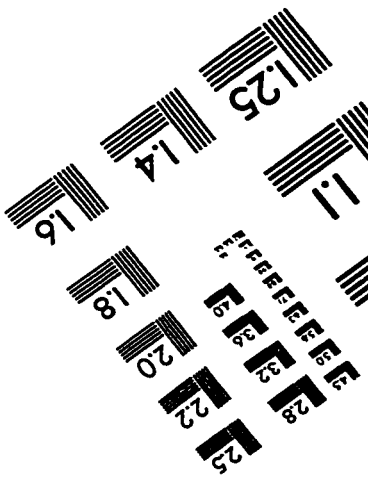












APPLIED IMAGE, Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989