

Topics in Algebra and Number Theory with
Applications to Abelian Difference Sets

S. E. Payne

June 27, 2005

Contents

| | | |
|----------|--------------------------------------------------|-----------|
| 1 | Some Basic Algebra | 7 |
| 1.1 | Characters of Finite Abelian Groups | 7 |
| 1.2 | Algebra Over Finite Fields | 9 |
| 1.3 | Abelian Difference Sets | 13 |
| 1.4 | The Group Ring | 18 |
| 1.5 | Some p -adic Computations | 23 |
| 1.6 | Hyperovals | 29 |
| 1.7 | The Transfer Matrix Method | 32 |
| 1.8 | Linear Recurrences | 35 |
| 1.9 | Multiplier Theory | 36 |
| | | |
| 2 | Algebraic Number Theory | 41 |
| 2.1 | Discriminants of Number Fields | 41 |
| 2.2 | Algebraic Integers | 46 |
| 2.3 | Ramification and Degree | 56 |
| | | |
| 3 | Cyclotomic Fields | 61 |
| 3.1 | Roots of Unity | 61 |
| 3.2 | Algebra in D_m | 63 |
| | | |
| 4 | Gauss Sums and the Stickelberger Relation | 71 |
| 4.1 | The Norm of an Ideal | 71 |
| 4.2 | An Additive Character on F | 72 |
| 4.3 | The Power Residue Symbol | 73 |
| 4.4 | Some Special Gauss and Jacobi Sums | 75 |
| 4.5 | Factoring Ideals in D_m | 80 |
| 4.6 | The Teichmüller Character | 81 |
| 4.7 | Stickelberger's Theorem at Last | 82 |

| | | |
|----------|-----------------------------------------------------------------|------------|
| 5 | Some Difference Sets and Their p-Ranks | 91 |
| 5.1 | The Singer Difference Sets | 91 |
| 5.2 | Monomial Hyperovals and Difference Sets | 97 |
| 5.3 | p -Ranks of The Segre Hyperovals $D(x^6)$ | 100 |
| 5.4 | p -Ranks of the Glynn Hyperovals $D(x^{3\sigma+4})$ | 102 |
| 5.5 | The Inequivalence of Certain Difference Sets | 111 |
| 6 | Notes by Carey Jenkins on Theorem 1.5.8 | 113 |
| 6.1 | Solving $S(a)+S(5a)=S(6a)+1$ | 113 |

PREFACE

During the spring semester of 2005 we offered a topics course Math 7023, at CU-Denver, whose goal was to read large parts of the paper "Gauss sums, Jacobi sums, and p -ranks of cyclic difference sets," *Jour. Comb. Theory (A)* 87(1999), 74 – 119, by R. Evans, H. Hollmann, C. Krattenthaler and Q. Xiang. This paper is deep, fundamental, and deserving of study. However, the students in this course needed to be introduced to many ideas and results before we could proceed directly to the paper. Hence these notes were developed. In general we hope to give the reader some facility with certain algebraic tools that might prove to be useful in further mathematical investigations. This has led to the inclusion of certain results and their proofs that are not actually needed in working through the paper by Evans et al., even though in general our goal was to include just what was needed to work through that paper. Particularly in the sections dealing with basic algebraic number theory we have made some attempt to go only as far as it appears to be necessary to read the paper cited. This is usually because the proofs are shorter or simpler in these cases and allow us to get to the paper itself sooner.

Our two favorite books on algebraic number theory for beginners are:

K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, Springer-Verlag, 1993.

and

P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.

From time to time we mention results without proof, but we have endeavored to prove everything that lies beyond the usual beginning graduate algebra course and is actually used here. A major result which is proved here is Stickelberger's Theorem on the factorization of a certain Gauss sum in a cyclotomic extension of the rationals.

We would particularly like to thank the students whose participation made this course possible and enjoyable: Stephen Flink, Carey Jenkins, Ryan Pedersen and Rob Rostermundt.

Chapter 1

Some Basic Algebra

1.1 Characters of Finite Abelian Groups

Let G be a finite abelian group written multiplicatively. We assume the reader is familiar with the fundamental theorem that says that G may be written as the direct product of cyclic groups $C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}$, where C_d is cyclic of order d , and d_i divides d_{i+1} , $1 \leq i < k$. A proof of this result is contained in most abstract algebra texts.

A *character* of G is a homomorphism χ from G into the multiplicative group F^* of some field F , often the field \mathcal{C} of complex numbers. If G has order v and exponent m , we usually want F to contain a primitive m th root of unity, but in any case we always want $|G| \neq 0 \in F$. If the field F is understood, we denote the set of all characters of G into F^* by \hat{G} . If χ_1 and χ_2 are two characters of G , their product $\chi_1\chi_2$ is the function sending g to $\chi_1(g)\chi_2(g)$. Clearly the product of two characters is again a character, and this product makes \hat{G} into an abelian group. The identity of \hat{G} is called the *principal character* or the *trivial character* and is usually denoted by χ_0 . Clearly $\chi_0(g) = 1$ for all $g \in G$.

Lemma 1.1.1. *Let $\chi \in \hat{G}$ with values in F^* . Then*

- (i) $\chi(e) = 1$, if e is the identity of G .
- (ii) $\chi(g^{-1}) = \chi(g)^{-1}$. If $F^* = \mathcal{C}^*$, then $\chi(g^{-1}) = \overline{\chi(g)}$.

Proof. All but the last equality of part (ii) follow immediately from the fact that χ is a group homomorphism. If $\chi(g) \in \mathcal{C}$, then it is a complex root of unity, so its multiplicative inverse must also be its complex conjugate, which proves the last equality. \square

Theorem 1.1.2. *For any finite abelian group G , $G \cong \hat{G}$.*

Proof. The proof is by induction on the order $|G|$ of G . If G is cyclic of order m with generator g , then each character of G is determined by its action on g . Then since g has order m , $\chi(g)^m = 1$. Hence $\chi(g)$ is an m th root of unity. If w is a fixed primitive m th root of unity, then the characters of G are all determined by equations of the form $\chi_r(g) = w^r$. There are m choices of r , so m characters. They are all powers of χ_1 , so \hat{G} is cyclic of order m .

Now suppose that $G = G_1 \times G_2$ where G is not cyclic. We will show that $\hat{G} \cong \hat{G}_1 \times \hat{G}_2$. The result will then follow by induction. (Note that this proof does not actually use the fundamental theorem on finite abelian groups.) Map \hat{G} into $\hat{G}_1 \times \hat{G}_2$ by sending χ to $(\chi|_{G_1}, \chi|_{G_2})$. Then map $\hat{G}_1 \times \hat{G}_2$ to \hat{G} by identifying (χ_1, χ_2) with the character sending (g_1, g_2) to $\chi_1(g_1)\chi_2(g_2)$. It is easy to check that these maps are both homomorphisms and are inverses of each other, so both are isomorphisms. \square

Corollary 1.1.3. *G is naturally isomorphic to $\hat{\hat{G}}$ by letting the element $g \in G$ correspond to the character (“evaluation at g ”): $\chi \mapsto \chi(g)$ on \hat{G} .*

Proof. The indicated correspondence is a homomorphism of G into $\hat{\hat{G}}$. If it is one-to-one then they are isomorphic, since they have the same order by Theorem 1.1.2. Suppose the kernel of this homomorphism is the subgroup H . Then for any character χ of G we have $\chi(h) = 1$ for all $h \in H$. This means that χ can be viewed as a character on G/H . Then $|G| = |\hat{G}| \leq |G|/|H|$, implying that $|H| = 1$ as needed. \square

Theorem 1.1.4. *(Orthogonality relations)*

$$(i) \sum_{g \in G} \chi_1(g)\chi_2(g) = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2^{-1}, \\ |G| & \text{if } \chi_1 = \chi_2^{-1}. \end{cases}$$

$$(ii) \sum_{\chi \in \hat{G}} \chi(g)\chi(h) = \begin{cases} 0 & \text{if } gh \neq e, \\ |G| & \text{if } gh = e. \end{cases}$$

Proof. Let χ denote a nonprincipal character and h some element of G with $\chi(h) \neq 1$. Then

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(gh) = \chi(h) \sum_{g \in G} \chi(g).$$

Since $\chi(h) \neq 1$ it must be that $\sum_{g \in G} \chi(g) = 0$. Now if $\chi = \chi_1\chi_2$ the first alternative of (i) is proved. The second alternative is obvious since

$\chi_1(g)\chi_1^{-1}(g) = 1$ for each $g \in G$. To prove part (ii), just use the identification of G with \hat{G} and use part (i) with \hat{G} in place of G . \square

An interesting special case of part (i) of the preceding theorem is when $\chi_2 = \chi_0 \neq \chi_1$.

Corollary 1.1.5. *If $\chi \neq \chi_0$, then $\sum_{g \in G} \chi(g) = 0$.*

In these notes the groups on which we study characters are the multiplicative and the additive subgroups of a finite field. So we briefly review some facts about finite fields and polynomials over them.

1.2 Algebra Over Finite Fields

If $q = p^e$, $e \geq 1$, with p a prime, there is a Galois field $F_q = GF(q)$ with q elements. Moreover, each finite field is isomorphic to some Galois field. We know that F_q contains $F_p = GF(p) \cong Z/pZ$ as its *prime subfield*. If $f(x)$ is an irreducible polynomial of degree e over F_p , then

$$F_q \cong F_p[x]/(f(x)) = \{a_0 + a_1t + \cdots + a_{e-1}t^{e-1} : a_i \in F_p \text{ and } f(t) = 0\}. \quad (1.1)$$

If F_r is a Galois field for some prime power r , then F_r contains an isomorphic copy of F_q as a subfield if and only if $r = p^h$ where e divides h . If F_q also denotes this subfield, then

$$F_q = \{a \in F_r : a^q = a\}. \quad (1.2)$$

We know that $F_q^* = F_q \setminus \{0\}$ is a cyclic group whose binary operation is just multiplication of F_q restricted to F_q^* . A generator of F_q^* is called a *primitive element* or *primitive root* for F_q .

The group $\text{Aut}(F_q)$ of automorphisms of F_q is cyclic of order e and generated by the automorphism

$$p : F_q \rightarrow F_q : x \mapsto x^p. \quad (1.3)$$

It follows that $\phi^i : x \mapsto x^{p^i}$.

Relative Trace and Norm

Let $q = p^e$ be any prime power and n any positive integer. Put $F = GF(q^n)$ and $K = GF(q)$. Then the *relative trace* $T_{F/K}(a)$ of an element $a \in F$ is defined by

$$T_{F/K}(a) = a + a^q + a^{q^2} + \cdots + a^{q^{n-1}}.$$

Clearly $T_{F/K}(a) \in K$; $T_{F/K}(a + b) = T_{F/K}(a) + T_{F/K}(b)$ for all $a, b \in F$; and for $c \in K$, $a \in F$, $T_{F/K}(ca) = cT_{F/K}(a)$. If $e = 1$, so q is prime, then $T_{F/K}$ is the *absolute trace function*. If $a \in K$, then $T_{F/K}(a) = na = 0$ if $n \equiv 0 \pmod{p}$. Note that $T_{F/K}$ is a K -linear transformation of the field F thought of as an n -dimensional vector space over K .

For the rest of this section let us write $tr(a) = T_{F/K}(a)$ for $a \in F$. And for $\sigma \in Gal(F/K)$, define $T_\sigma \in Hom_K(F, F)$ by $T_\sigma(a) = a^\sigma - a$ for all $a \in F$. It is easy to check that $tr(T_\sigma(a)) = 0$ for all $a \in F$. So $Im(T_\sigma) \subseteq ker(tr)$. First suppose that σ generates $Gal(F/K)$, so that K is the subfield fixed by σ . In this case K is exactly the kernel of T_σ , so that the image of T_σ has $q^n/q = q^{n-1}$ elements. This is a vector subspace of F of codimension 1 over K . Since tr is not the zero map (a polynomial of degree q^{n-1} cannot have more than q^{n-1} roots in F), it must be that $tr(b) = 0$ if and only if $b = T_\sigma(a)$ for some $a \in F$. This holds for each σ that generates the Galois group $Gal(F/K)$. Now suppose that $\sigma \in Gal(F/K)$ has fixed field larger than K , so that the kernel of T_σ is larger than K , say it is $GF(q^j)$ with $1 < j \leq n$. Then the image of T_σ has only q^{n-j} elements in it, so that it is a proper subset of the kernel of $tr = T_{F/K}$. We have proved the following result.

Theorem 1.2.1. *Let σ be a generator of the Galois group $Gal(F/K)$. Then $tr(b) = T_{F/K}(b) = 0$ if and only if $b = T_\sigma(a) = a^\sigma - a$ for some $a \in F$.*

At one point later on we need the following result.

Theorem 1.2.2. *Let E/F and F/K be finite extensions of finite fields, so that each of E/F , F/K and E/K is a Galois extension. Then $T_{E/K} = T_{F/K} \circ T_{E/F}$.*

Proof. The proof of the result in this special case is an easy exercise. \square

The *relative norm* $N_{F/K}$ of an element $a \in F$ is defined by

$$N_{F/K}(a) = a^{1+q+q^2+\cdots+q^{n-1}} = a^{\frac{q^n-1}{q-1}}.$$

Clearly $N_{F/K}(a) \in K$, and if $a = b^{q-1}$ then $N_{F/K}(a) = 1$. The kernel of $x \mapsto x^{q-1}$ in F^* is K^* , so the size of the image I of the map $x \mapsto x^{q-1}$ is $\frac{q^n-1}{q-1}$, and I is a subset of the kernel of the map $x \mapsto x^{\frac{q^n-1}{q-1}}$ which has size $\frac{q^n-1}{q-1}$. Hence we have proved

Theorem 1.2.3. $N_{F/K}(a) = 1$ if and only if $a = b^{q-1}$ for some $b \in F$.

Polynomials over F_q

If $q = 2$, then $x^q + x = x(x+1) = x^2 + (0+1)x$, and $\sum_{a \in F_2} a = 1$. For the remainder of this section let $q > 2$, so that x^q, x^{q-1}, x are distinct monomials.

$$x^q - x = \prod_{a \in F_q} (x - a), \quad (1.4)$$

from which it follows that

$$x^{q-1} - 1 = \prod_{a \in F_q^*} (x - a) = x^{q-1} - \left(\sum_{a \in F_q^*} \right) x^{(q-2)} + \cdots + (-1)^{q-1} \prod_{a \in F_q^*} a. \quad (1.5)$$

From Eq 1.5 we see immediately that

$$\sum_{a \in F_q^*} a = \sum_{a \in F_q} a = 0; \quad \prod_{a \in F_q^*} a = (-1)^q = -1. \quad (1.6)$$

Note: For fixed $a \in F_q$,

$$\prod_{\substack{b \in F_q \\ b \neq a}} (a - b) = \prod_{b \in F_q^*} b = (-1)^q = -1. \quad (1.7)$$

Put $\Gamma[x] = F_q[x]/(x^q - x)$ and $G(x) = \{f(x) \in F_q[x] : \deg(f(x)) \leq q-1\}$. Then each $g(x) \in F_q[x]$ has a unique coset representation in $G(x)$. Moreover, if $g(x) \in F_q[x]$ and $f(x) \in G(x)$, then

$$f(a) = g(a) \text{ for all } a \in F_q \text{ iff } f(x) \equiv g(x) \pmod{x^q - x}. \quad (1.8)$$

Put

$$\delta_{a,b} = \begin{cases} 1, & \text{if } a = b; \\ 0, & \text{if } a \neq b. \end{cases}$$

Recall *Lagrange interpolation*. For $a \in F_q$, put

$$f_a(x) = \frac{x^q - x}{(x - a)(-1)^q} = \frac{\prod_{\substack{b \in F_q \\ b \neq a}} (x - b)}{\prod_{\substack{b \in F_q \\ b \neq a}} (a - b)}. \quad (1.9)$$

Then $f_a(b) = \delta_{a,b}$ for all $a, b \in F_q$. Let $h : F_q \rightarrow F_q$ be any function. Put

$$f(x) = \sum_{a \in F_q} h(a) f_a(x). \quad (1.10)$$

Then

$$f(b) = \sum_{a \in F_q} h(a) f_a(b) = h(b), \text{ for all } b \in F_q. \quad (1.11)$$

This shows that each function $h : F_q \rightarrow F_q$ is a polynomial function f . But we want to write $f(x) = \sum_{r=0}^{q-1} a_r x^r$ where a_r is given in terms of functional values.

Theorem 1.2.4. *Let $h : F_q \rightarrow F_q$ be any function. Then there is a polynomial $f(x) = \sum_{r=0}^{q-1} a_r x^r$ for which $f(b) = h(b)$ for all $b \in F_q$. Moreover,*

$$(i) \ a_0 = f(0) = h(0);$$

$$(ii) \ a_{q-1} = -\sum_{a \in F_q} h(a);$$

$$(iii) \ \text{For } 0 < r < q-1, \ a_r = -\sum_{a \in F_q^*} h(a) a^{-r}.$$

Proof. Put $x = 0$ in Eq. 1.10 to see that $h(0) = f(0) = a_0$. Next, the coefficient on x^{q-1} in $f_a(x)$ is $(-1)^q = -1$ (for q odd or even). Hence from Eq. 1.10, $a_{q-1} = -\sum_{a \in F_q} h(a)$. Now suppose $0 < r < q-1$. If $a = 0$, the coefficient on x^r in $\frac{x^q - x}{x - a} = x^{q-1} - 1$ is zero. If $a \neq 0$, put $b(x) = \frac{x^q - x}{x - a} = b_0 + b_1 x + \cdots + b_{q-1} x^{q-1} = 0 + b_1 x + \cdots + b_{q-2} x^{q-2} + x^{q-1}$. So

$$\begin{aligned} x^q - x &= (x - a)(b_1 x + \cdots + b_{q-2} x^{q-2} + x^{q-1}) \\ &= (-ab_1)x + (b_1 - ab_2)x^2 + (b_2 - ab_3)x^3 + \cdots + (b_{q-2} - ab_{q-1})x^{q-1} + x^q. \end{aligned}$$

This implies $ab_1 = 1$, or $b_1 = a^{-1}$. And $0 < r < q-1$ forces $b_{r-1} - ab_r = 0$, or $b_r = a^{-r}$. So $b_1 = a^{-1}$; $b_2 = b_1 a^{-1} = a^{-2}$; $b_3 = b_2 a^{-1} = a^{-3}$, ..., and $b_r = a^{-r}$. So the coefficient of x^r in $f_a(x)$ is 0 if $a = 0$ and $-a^{-r}$ if $a \neq 0$. By Eq. 1.10, the coefficient on x^r is $a_r = -\sum_{a \in F_q^*} h(a) a^{-r}$. \square

Lemma 1.2.5. *Assume $q > 2$ and suppose $f(x) \in G(x)$. If $a \mapsto f(a)$ is a bijection, then $\deg(f(x)) \leq q - 2$.*

Proof. By assumption, $\sum_{a \in F_q} f(a) = \sum_{a \in F_q} a = 0$, since $q > 2$. So the coefficient on x^{q-1} is $-\sum_{a \in F_q} f(a)$, which is 0. \square

Lemma 1.2.6. *Let $q > 2$ and let $f(x)$ permute the nonzero elements of F_q . If $\deg(f(x)) \leq q - 2$, it must be that $f(0) = 0$ and $a \mapsto f(a)$ is a bijection on F_q .*

Proof. From Eq. 1.10 we have $f(x) = -\sum_{a \in F_q} f(a) \left(\frac{x^q - x}{x - a}\right) = -f(0)(x^{q-1} - 1) - \sum_{a \in F_q^*} f(a) \left(\frac{x^q - x}{x - a}\right)$. The coefficient of x^{q-1} , which must be 0, is $-f(0) - \sum_{a \in F_q^*} f(a) = -f(0) - \sum_{a \in F_q^*} a = -f(0)$. Hence $f(0) = 0$ and $a \mapsto f(a)$ is a bijection. \square

1.3 Abelian Difference Sets

We start with a definition of symmetric block design that is apparently more restrictive than the usual definition, but in fact they are equivalent. Our goal here is only to present a small bit of the theory that relates to difference sets.

A *symmetric (v, k, λ) -design* $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ is a set P of v points together with a set of v distinct subsets called *blocks* satisfying the following properties:

- (i) Each block has k points and each point is in k blocks.
- (ii) Each pair of distinct points lie in λ blocks and each pair of blocks intersect in a set of λ points.

Given a symmetric block design with ordered pointset $\mathcal{P} = \{x_1, \dots, x_v\}$ and ordered block set $\mathcal{B} = \{B_1, \dots, B_v\}$, the *incidence matrix* N is defined by

$$N = (n_{ij}), \quad \text{where } n_{ij} = 1 \text{ if } x_i \in B_j \text{ and } n_{ij} = 0 \text{ otherwise.}$$

One of the fundamental results is that N is invertible, but we leave the proof of this result to the reader. (For example, it follows from Theorem 19.7 of van Lint and Wilson.)

Sometimes we also use the notation $n_{ij} = N(x_i, B_j)$ or just $N(x, B)$. An automorphism of \mathcal{S} is a pair $\alpha = (P, Q)$ of permutations where P is a permutation of the points and Q is a permutation of the blocks such that $x \in B$ if and only if $P(x) \in Q(B)$. Here we may identify P with the

permutation matrix whose rows and columns are indexed by the points of \mathcal{S} and

$$P(x, y) := \begin{cases} 1 & \text{if } \alpha(x) = y, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, we may identify Q with the permutation matrix whose rows and columns are indexed by the blocks of \mathcal{S} and

$$Q(A, B) := \begin{cases} 1 & \text{if } \alpha(A) = B, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the trace of P is equal to the number of fixed points, and the trace of Q is equal to the number of fixed blocks of α . Now we have

$$PNQ^T(x, A) = \sum_{y \in \mathcal{P}; B \in \mathcal{B}} P(x, y)N(y, B)Q(A, B) = N(\alpha(x), \alpha(A)) = N(x, A).$$

This says that $PNQ^T = N$. Equivalently, $P = NQN^{-1}$. Thus P and Q , being similar matrices, have the same trace and we have proved the following theorem.

Theorem 1.3.1. *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ be a symmetric (v, k, λ) -design with $0 < \lambda < k < v$, and let α be an automorphism of \mathcal{S} . Then the number of points fixed by α is equal to the number of blocks fixed by α .*

Corollary 1.3.2. *The type of the cycle decomposition of α on the point set \mathcal{P} is the same as the type of the cycle decomposition of α on the block set \mathcal{B} .*

Proof. By Theorem 1.3.1, α^i has the same number of fixed points as fixed blocks, for each $i = 1, 2, \dots$

Suppose a permutation β has c_i cycles of length i on some set S , $i = 1, 2, \dots, |S|$. Let f_j denote the number of fixed points of β^j . Then after a little thought we see that

$$f_j = \sum_{i|j} ic_i,$$

and by Möbius inversion,

$$jc_j = \sum_{i|j} \mu\left(\frac{j}{i}\right) f_i.$$

The point is that the numbers of cycles of each length (i.e., the type of β) are determined completely by the numbers of fixed points of the powers of β . \square

Corollary 1.3.3. *If G is a group of automorphisms of a symmetric design, then the number of orbits of G on the point set \mathcal{P} is the same as the number of orbits of G on the block set \mathcal{B} . In particular, G is transitive on the points if and only if G is transitive on the blocks.*

Proof. By the orbit counting lemma, the number of orbits of a group G of permutations of a set S is determined exactly by the multiset $(f(\alpha) : \alpha \in G)$ where $f(\alpha)$ is the number of elements of S fixed by α . \square

Let G be an (additive) abelian group of order v . A (v, k, λ) -*difference set* in G is a k -subset $D \subseteq G$ such that each nonzero $g \in G$ occurs exactly λ times in the multiset $(x - y : x, y \in D)$ of differences from D . More formally, we are requiring that the number of ordered pairs (x, y) with $x, y \in D$ and $x - y = g$ be λ when $g \neq 0$ and this number is k for $g = 0$. It is easy to see that $\lambda(v - 1) = k(k - 1)$. A difference set is *nontrivial* when $1 < k < v - 1$ (which implies $0 < \lambda < k$). A difference set with $\lambda = 1$ is called *planar* or *simple*.

Let D be a k -subset of the abelian group G of order v . For $g \in G$, we denote by $D + g$ the *translate* or *shift*,

$$D + g := \{x + g : x \in D\}$$

of D by g . For $x, y \in G$ we claim that the number of shifts $D + g$ that contain both x and y is equal to the number of times $d := x - y$ occurs as a difference within D . This is because $g \mapsto (x - g, y - g)$ is a one-to-one correspondence between the set $\{g \in G : \{x, y\} \subseteq D + g\}$ and the set of ordered pairs (a, b) of elements of D such that $a - b = x - y$. It is also an easy exercise to check that this common number is also equal to the cardinality of the intersection $(D + x) \cap (D + y)$.

In particular, $(G, \{D + g : g \in G\})$ is a symmetric (v, k, λ) -design if and only if D is a (v, k, λ) -difference set. The design $(G, \{D + g : g \in G\})$ is called the *development* of the difference set D .

In the above discussion using abelian groups the term *difference set* is appropriate because the definition refers to the set of *differences* of elements of D . If the group G is written multiplicatively, especially if it is not even

abelian, it makes more sense to talk about *quotient sets*. For much of our later discussion we need to write the group multiplicatively, so we give here the alternative definition and just do it for general groups.

A (v, k, λ) -*quotient set* in an arbitrary group G of order v (written multiplicatively) is a k -subset $D \subset G$ such that any one of the following conditions holds:

Each nonidentity element $g \in G$ occurs exactly λ times

$$\text{in the list } (x^{-1}y : x, y \in D) \text{ of "left" quotients from } D. \quad (1.12)$$

Each nonidentity element $g \in G$ occurs exactly λ times

$$\text{in the list } (xy^{-1} : x, y \in D) \text{ of "right" quotients from } D. \quad (1.13)$$

$$|D \cap (Dg)| = \lambda \text{ for each nonidentity } g \in G. \quad (1.14)$$

$$|D \cap (gD)| = \lambda \text{ for each nonidentity } g \in G. \quad (1.15)$$

$$(G, \{Dg : g \in G\}) \text{ is a symmetric } (v, k, \lambda) \text{ - design.} \quad (1.16)$$

$$(G, \{gD : g \in G\}) \text{ is a symmetric } (v, k, \lambda) \text{ - design.} \quad (1.17)$$

To see that Eqs. 1.12 through 1.17) are equivalent requires the following result: If S is a system of v points together with v blocks of k points such that any two distinct blocks intersect in λ points, then it must also be true that each point is in k blocks and any two points are together in exactly λ blocks. With this information, however, it becomes an elementary exercise to show that the conditions in Eqs. 1.12 through 1.17 are equivalent.

Exercise 1.3.3.1. *Work through the proof of Theorem 8.2.1 (and hence that of Theorem 8.2.2) of Ryser [Ry63], and then complete the proof that the conditions in Eqs. 1.12 through 1.17 are equivalent. (Hint: Consider the map $g \leftrightarrow g^{-1}D$.)*

Theorem 1.3.4. *Let G be a group of order v . The existence of a (v, k, λ) -quotient set in G is equivalent to the existence of a symmetric (v, k, λ) -design that admits a group \hat{G} of automorphisms that is isomorphic to G and regular, i.e., sharply transitive, on the points of the design.*

Proof. Let D be a (v, k, λ) -quotient set in G . Then $(G, \{gD : g \in G\})$ is a symmetric (v, k, λ) -design. For $g \in G$, define a permutation \hat{g} of G by $\hat{g}(x) = gx$. Then each \hat{g} is easily seen to be an automorphism of $(G, \{gD : g \in G\})$ and the group $\hat{G} = \{\hat{g} : g \in G\}$ of automorphisms is clearly isomorphic to G and regular on the points.

Conversely, let G be given and let $(\mathcal{P}, \mathcal{B})$ be a symmetric (v, k, λ) -design with regular group \hat{G} of automorphisms of $(\mathcal{P}, \mathcal{B})$ that is isomorphic to G . It will be sufficient to exhibit a (v, k, λ) -quotient set in \hat{G} .

Fix a point $x_0 \in \mathcal{P}$ and a block $B_0 \in \mathcal{B}$. Let

$$D := \{\sigma \in \hat{G} : \sigma(x_0) \in B_0\}.$$

We claim that D is a (v, k, λ) -quotient set in \hat{G} . Since \hat{G} is regular and $|B_0| = k$, we have $|D| = k$. Let α be a nonidentity element of \hat{G} . Then $\alpha D = \{\alpha\sigma : \sigma(x_0) \in B_0\} = \{\tau : \tau(x_0) \in \alpha(B_0)\}$, so

$$D \cap (\alpha D) = \{\tau : \tau(x_0) \in B_0 \cap \alpha(B_0)\}.$$

Since \hat{G} is regular, α has no fixed points and hence, by Theorem 1.3.1, fixes no block. Thus the block $\alpha(B_0)$ is distinct from B_0 , so $|B_0 \cap \alpha(B_0)| = \lambda$, and by regularity, $|D \cap (\alpha D)| = \lambda$. This holds for all nonidentity elements α and establishes our claim. \square

For example, the existence of a *cyclic* (v, k, λ) -difference set, i.e., a difference in the cyclic group \mathcal{Z}_v , is equivalent to the existence of a symmetric (v, k, λ) -design that admits a cyclic automorphism, i.e., an automorphism with cycle decomposition on the points – or blocks – consisting of one cycle of length v .

From now on we restrict our attention to difference sets or quotient sets in abelian groups.

The following lemma has an easy proof.

Lemma 1.3.5. *$D \subset G$ is a (v, k, λ) -difference set if and only if $G \setminus D$ is a $(v, v - k, v - 2k + \lambda)$ -difference set. Also, D is a difference set if and only if every translate of D is a difference set.*

In the case that $(v, k) = 1$ it happens that we can choose a natural representative from the class of all translates. Call a subset of an additively

written abelian group G *normalized* in the case that the sum of its elements is zero.

Lemma 1.3.6. *Let D be a k -subset of an abelian group F of order v . If $(v, k) = 1$, then D has a unique normalized translate.*

Proof. Let h be the sum of the elements of D . Then the sum of the elements of a translate $D + g$ is $h + kg$. Since $(v, k) = 1$, there are integers s and t such that $sk + tv = 1$. Put $g = -sh$. Then $h + kg = h + k(-sh) = (1 - sk)h = tvh = 0$. So $D + g$ is normalized. Suppose $h + kg_1 = h + kg_2 = 0$. Then $k(g_1 - g_2) = 0$. But k is relatively prime to the order of any element of G (which must divide v), so we must have $g_1 = g_2$. \square

Now suppose that G is a finite abelian group written multiplicatively and with order v , and suppose that D_1 and D_2 are (v, k, λ) -quotient sets in G . We say D_1 and D_2 are *equivalent* (written $D_1 \cong D_2$) provided there is an automorphism α of G and an element a of G for which

$$D_1^{(\alpha)} := \{d^\alpha : d \in D_1\} = D_2 \cdot a := \{da : d \in D_2\}.$$

It is routine to check that if $D_1 \cong D_2$, then the symmetric block designs derived from the two quotient sets are equivalent. Note also that if G is cyclic, then $D_1 \cong D_2$ iff there is a $t \in \mathcal{Z}$ with $(t, v) = 1$ and there is an $a \in G$ with $D_1 = D_2^{(t)} \cdot a$.

Also note that if G is written multiplicatively and D is a k -subset of G with $(k, v) = 1$, the unique “translate” $D \cdot a$ of D that is normalized is the one with $\prod_{d \in D} (da) = e$, the multiplicative identity of G .

1.4 The Group Ring

Let R be a ring with $1 \neq 0$ and let $G = \{g_1, \dots, g_n\}$ be any finite group with group operation written multiplicatively. Define the *group ring*, $R[G]$, of G with coefficients in R to be the set of all formal sums

$$a_1g_1 + a_2g_2 + \dots + a_ng_n, \quad a_i \in R, \quad 1 \leq i \leq n.$$

If g_1 is the identity of G we shall write a_1g_1 simply as a_1 . Similarly, we shall write the element $1g$ for $g \in G$ simply as g .

Addition is defined “componentwise”:

$$(a_1g_1 + \cdots + a_ng_n) + (b_1g_1 + \cdots + b_ng_n) = (a_1 + b_1)g_1 + \cdots + (a_n + b_n)g_n.$$

Multiplication is performed by first defining $(ag_i)(bg_j) = (ab)g_k$, where the product ab is taken in R and $g_i g_j = g_k$ is the product in G . This product is then extended to all formal sums by the distributive laws, so that the coefficient of g_k in the product

$$(a_1g_1 + \cdots + a_ng_n) \times (b_1g_1 + \cdots + b_ng_n)$$

is $\sum_{g_i g_j = g_k} a_i b_j$.

It is routine to check that these operations make $R[G]$ into a ring with $1 \neq 0$. The associativity of multiplication follows from the associativity of the group operation in G . The ring $R[G]$ is commutative if and only if R is a commutative ring and G is a commutative group. Suppose that R is commutative with G a finite group $G = \{g_1, \dots, g_n\}$. The map from the group ring $R[G]$ to R defined by $\iota : \sum_{i=1}^n a_i g_i \mapsto \sum_{i=1}^n a_i$ is easily seen to be a homomorphism, called the *augmentation map*. The kernel of the augmentation map, the *augmentation ideal*, is the set of elements of $R[G]$ whose coefficients sum to 0. For example, $g_i - g_j$ is an element of the augmentation ideal for all i, j . Since the augmentation map is surjective, the quotient ring is isomorphic to R .

In these notes we will usually take R to be the commutative ring \mathcal{C} of complex numbers, the subring \mathcal{Z} of rational integers, some subfield of \mathcal{C} or a finite field.

For a subset $B \subset G$, we identify B with $\sum_{g \in B} g$. Then for $A, B \subset G$, $AB = \sum_{g \in G} c_g g$ where c_g is the number of times g occurs in the multiset $(g_1 g_2 : g_1 \in A, g_2 \in B)$ of products of elements in A and B . For $A = \sum_{g \in G} a_g g$ write $A^{-1} = \sum_{g \in G} a_g g^{-1} = \sum_{g \in G} a_{g^{-1}} g$.

For a k -subset D of a group G of order v , D is a (v, k, λ) -quotient set in G with $n := k - \lambda$ if and only if the equation

$$DD^{-1} = n + \lambda G \tag{1.18}$$

holds in the group ring $\mathcal{Z}[G]$.

Here by n we mean ne where e is the identity element of G and n is the ordinary integer $n \in \mathcal{Z}$.

Theorem 1.4.1. *Let v, k, λ be positive integers such that*

$$\lambda(v - 1) = k(k - 1),$$

and let G be an abelian (multiplicative) group of order v . The existence of a (v, k, λ) -quotient set in G is equivalent to the existence of an element $A \in \mathcal{Z}[G]$ satisfying the equation

$$AA^{-1} = n + \lambda G, \text{ where } n := k - \lambda. \quad (1.19)$$

Proof. We have already seen that if D is a subset of G , then D satisfies Eq. 1.18 if and only if D is a (v, k, λ) -quotient set. It remains to show that if there is a solution $A \in \mathcal{Z}[G]$ to Eq. 1.19, then we can find a solution $B = \sum_{g \in G} b_g g$ where the coefficients b_g are 0's and 1's.

Assume that A satisfies Eq. 1.19 and apply the augmentation map ι from $\mathcal{Z}[G] \rightarrow \mathcal{Z}$. Write $\iota : A \mapsto A_0 \in \mathcal{Z}$. We find that (since $\iota(A) = \iota(A^{-1})$) equating the images of ι on the two sides of Eq. 1.19 yields

$$(A_0)^2 = n + \lambda v = k^2, \text{ so } A_0 = \pm k.$$

Since A satisfies Eq. 1.19, so does $B = -A$, so we may assume $A_0 = \sum a_g = k$.

The coefficient of 1 in AA^{-1} is $k = \sum_{g \in G} a_g^2$. Thus $\sum_{g \in G} a_g(a_g - 1) = 0$. But $a(a - 1)$ is strictly positive unless the integer a is 0 or 1, hence each coefficient a_g in A is 0 or 1. \square

Note: The above proof shows that if A is a solution to Eq. 1.19 then either A or $-A$ is a quotient set.

If $A = \sum_{g \in G} a_g g \in \mathcal{C}[G]$ and χ is any character on G , then $\chi(A) := \sum_{g \in G} a_g \chi(g)$. As a consequence of the orthogonality relations we get the so-called *Fourier inversion formula*.

Theorem 1.4.2. *If $A = \sum_{g \in G} a_g g \in \mathcal{C}[G]$, then*

$$a_h = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(Ah^{-1}) \text{ for all } h \in G.$$

Proof. $\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(Ah^{-1}) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi\left(\sum_{g \in G} a_g gh^{-1}\right) = \frac{1}{|G|} \sum_{g \in G} \left(\sum_{\chi \in \hat{G}} a_g \chi(gh^{-1})\right) = a_h$ by the orthogonality relations. \square

Corollary 1.4.3. *If $A \in \mathcal{Z}[G]$ satisfies $\chi(A) = 0$ for all nontrivial characters χ of G , then $A = mG$ for some integer m .*

Proof. For each $h \in G$, $a_h = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(Ah^{-1}) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(A)\chi(h^{-1}) = \frac{1}{|G|} \chi_0(A)\chi_0(h^{-1}) = \frac{a(A)}{|G|}$, which is a constant m independent of h . But $m \in \mathcal{Z}$ since $A \in \mathcal{Z}[G]$ by hypothesis. \square

Theorem 1.4.4. *A k -subset D of G is a (v, k, λ) -quotient set in G if and only if (in $\mathcal{Z}[G]$)*

$$\chi(D)\overline{\chi(D)} = n = k - \lambda \text{ for every nontrivial character } \chi \text{ of } G.$$

Proof. First assume that $DD^{-1} = (k - \lambda)1 + \lambda G$. Then for $\chi \neq \chi_0$, $\chi(D)\overline{\chi(D)} = \chi(D)\chi(D^{-1}) = \chi(DD^{-1}) = \chi(k - \lambda) + \chi(\lambda G) = k - \lambda + \lambda\chi(G) = k - \lambda$, where the last equality follows from part (i) of Theorem 1.1.4 with $\chi_2 = \chi_0$. For the converse assume that $\chi(D)\overline{\chi(D)} = k - \lambda$ for all characters $\chi \neq \chi_0$. Put $A = DD^{-1} - (k - \lambda)1 - \lambda G$. For $\chi \neq \chi_0$, $\chi(A) = (k - \lambda) - (k - \lambda) - 0 = 0$. Hence by Corollary 1.4.3 $A = mG$ for some m . Comparing coefficients of 1 we see that $m = k - (k - \lambda) - \lambda = 0$, forcing $DD^{-1} = (k - \lambda)1 + \lambda G$. Hence D is a quotient set by Theorem 1.4.1. \square

We note that the group ring $R[G]$ is a free R -module of rank $|G|$ and the addition in the group ring and the scalar multiplication is that of the module structure (here a left module). The group ring has a canonical involution given by extending the function $g \mapsto g^{-1}$ of G onto G to a function from $R[G]$ to $R[G]$ via

$$\sum_{g \in G} a_g g \mapsto \overline{\sum_{g \in G} a_g g},$$

where

$$\overline{\sum_{g \in G} a_g g} = \sum_{g \in G} a_g g^{-1} = \sum_{g \in G} a_{g^{-1}} g.$$

It follows that $\overline{\overline{A}} = A^{-1}$.

Exercise 1.4.4.1. *This involution of $R[G]$ has the usual properties: for any x and y in $R[G]$*

$$\overline{\overline{x}} = x; \quad \overline{x + y} = \overline{x} + \overline{y}; \quad \text{and } \overline{x \cdot y} = \overline{y} \cdot \overline{x}.$$

Any character $\chi : G \rightarrow F^*$ extends to a ring homomorphism of $\mathcal{Z}[G]$ into F via

$$\chi \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g \chi(g).$$

Also, for any character χ we define $\bar{\chi}$ by $\bar{\chi}(g) = \chi(g^{-1})$, or, equivalently (on the group ring) $\bar{\chi}(x) = \chi(\bar{x})$. This is a direct generalization of using conjugation in the classical case where F is the field of complex numbers, since then the complex conjugate of $\chi(g)$ is $(\chi(g))^{-1} = \chi(g^{-1})$. It is easy to check that $\bar{\chi}$ is also a character which is in fact χ^{-1} .

Let G be an abelian group (written multiplicatively) of order v and with exponent v^* . Let F be a field of characteristic p not dividing v which contains the v^* th roots of unity. Finally, let $B = \sum_{g \in G} b_g g$ be an element of the group algebra $F[G]$. Suppose $G = \{g_1, \dots, g_v\}$. Associate with B the matrix (b_{ij}) where

$$b_{ij} = b_{g_i g_j^{-1}}.$$

The rank of (b_{ij}) is called the *rank of B* . Let $(\chi(g))$ be the $v \times v$ matrix whose rows are labeled by the v characters $\chi : G \rightarrow F^*$ and whose columns are labeled by the v elements $g \in G$, so that the entry in row χ and column g is $\chi(g)$.

Lemma 1.4.5. *The matrix $(\chi(g))$ is nonsingular because it satisfies*

$$M := \frac{1}{v} (\chi(g)) \cdot (\chi(g^{-1}))^T = I_v.$$

Proof. Just for this proof let the characters from G into F^* be χ_1, \dots, χ_v . The (i, l) entry of M is

$$\frac{1}{v} \sum_j \chi_i(g_j) \chi_l^{-1}(g_j) = \begin{cases} 0 & \text{if } \chi_i \neq (\chi_l^{-1})^{-1} = \chi_l; \\ 1 & \text{if } \chi_i = \chi_l. \end{cases}$$

□

Put $\chi(B) = \sum_{g \in G} b_g \chi(g)$.

Lemma 1.4.6.

$$(\chi(g))(b_{ij})(\chi(g^{-1}))^T = v \cdot \text{diag}(\chi_1(B), \dots, \chi_v(B)).$$

Proof. First note that $\chi(g^{-1}) = \chi(g)^{-1} = \chi^{-1}(g)$. Then the (i, l) entry of the product on the left is

$$\begin{aligned}
& \sum_{j,k} \chi_i(g_j) \cdot b_{jk} \cdot \chi_l(g_k^{-1}) = \\
& \sum_{j,k} \chi_i(g_j) \chi_l(g_k^{-1}) \cdot b_{g_j g_k^{-1}} = \\
& \sum_{g \in G} b_g \left(\sum_j \chi_i(g_j) \chi_l(g_j^{-1} g) \right) = \\
& \sum_{g \in G} b_g \chi_l(g) \cdot \sum_j \chi_i(g_j) \chi_l(g_j^{-1}) = \\
& \sum_{g \in G} b_g \chi_l(g) \cdot \sum_j (\chi_i \chi_l^{-1})(g_j) = \\
& \chi_l(B) \cdot \begin{cases} v, & \text{if } i = l; \\ 0, & \text{if } i \neq l. \end{cases}
\end{aligned}$$

□

The following immediate corollary is due to MacWilliams and Mann.

Corollary 1.4.7. *The rank of B over F is equal to the number of characters $\chi : G \rightarrow F^*$ satisfying $\chi(B) \neq 0$.*

1.5 Some p -adic Computations

Let $q = p^f$ and let $a \in \mathcal{Z}$ with $0 \leq a < q - 1$. So a has a unique p -adic representation

$$a = \sum_{i=0}^{f-1} a_i p^i, \quad 0 \leq a_i \leq p - 1 \text{ for } 0 \leq i \leq f - 1.$$

Define $S(a) = \sum_{i=0}^{f-1} a_i$. Then for any integer $a \in \mathcal{Z}$ write $a = t(q - 1) + r$ with $0 \leq r < q - 1$. Put $S(a) = S(r)$ and write $L(a) = r$. So $L(x)$ is the reduction of x modulo $q - 1$, and $S(a)$ is the sum of the p -adic digits of the reduction modulo $q - 1$ of a .

Let $u \in \mathcal{R}$, the real numbers. Define $\langle u \rangle = u - [u]$ where $[u]$ is the *floor function* of u , i.e., it is the largest integer less than or equal to u . Hence $\langle u \rangle \in [0, 1)$ is the *fractional part* of u .

Lemma 1.5.1. $S(a) = (p-1) \sum_{i=0}^{f-1} \langle \frac{p^i a}{q-1} \rangle$.

Proof. Write $a = k(q-1) + r$, $0 \leq r < q-1$, and then $S(a) = S(r)$. Then

$$\begin{aligned} \langle \frac{p^i a}{q-1} \rangle &= \langle \frac{p^i(k(q-1) + r)}{q-1} \rangle = \\ &\langle p^i k + \frac{p^i r}{q-1} \rangle = \langle \frac{p^i r}{q-1} \rangle, \end{aligned}$$

so we may assume that $0 \leq a < q-1$. Writing the p -adic representation of a we have

$$a = \sum_{i=0}^{f-1} a_i p^i, \quad 0 \leq a_i < p.$$

Multiplying both sides of the equation by p and using the fact that $p^f = q \equiv 1 \pmod{q-1}$ we get

$$\begin{aligned} pa &= a_0 p + a_1 p^2 + \cdots + a_{f-2} p^{f-1} + a_{f-1} p^f \equiv \\ &= a_{f-1} + a_0 p + \cdots + a_{f-2} p^{f-1} \pmod{q-1}. \end{aligned} \tag{1.20}$$

Multiplying by p again and then proceeding inductively we find that

$$p^i a \equiv A_i =$$

$$a_0 p^i + a_1 p^{i+1} + \cdots + a_{f-i-1} p^{f-1} + a_{f-i} + a_{f-i+1} p + \cdots + a_{f-1} p^{i-1} \pmod{q-1}.$$

Since $0 \leq a_i < p$ the maximum value of the right hand side of the congruence is (setting $a_i = p-1$ for all i) $q-1$. However if this maximum were attained, then $a = q-1$, which is a contradiction. Thus the right hand sides of the congruences are all less than $q-1$.

Here $A_i = L(ap^i)$ where $L(x)$ is the reduction of the integer x modulo $q-1$. So

$$\langle \frac{ap^i}{q-1} \rangle = \langle \frac{A_i}{q-1} \rangle = \frac{A_i}{q-1} = \frac{L(ap^i)}{q-1}.$$

We now examine the sum

$$\sum_{i=0}^{f-1} \left\langle \frac{ap^i}{q-1} \right\rangle = \sum_{i=0}^{f-1} \frac{L(ap^i)}{q-1}.$$

Notice that as i runs through $0, 1, \dots, f-1$ each power of p is multiplied by each a_j just once. Hence we get

$$\sum_{i=0}^{f-1} \left\langle \frac{ap^i}{q-1} \right\rangle = \frac{S(a)(1+p+\dots+p^{f-1})}{q-1} = \frac{S(a)(p^f-1)}{(q-1)(p-1)} = \frac{S(a)}{p-1}.$$

This proves that

$$S(a) = (p-1) \sum_{i=0}^{f-1} \left\langle \frac{ap^i}{q-1} \right\rangle = \frac{p-1}{q-1} \sum_{i=0}^{f-1} L(ap^i). \quad (1.21)$$

□

Lemma 1.5.2. For $0 < a < q-1$, $S(pa) = S(a)$.

Proof. This is an immediate consequence of Eq. 1.20

□

Lemma 1.5.3. $\sum_{a=1}^{q-2} S(a) = \frac{f(p-1)(q-2)}{2}$.

Proof. Using the notation from above for the p -adic expansion of a , along with $q-1 = \sum_{i=0}^{f-1} (p-1)p^i$, we obtain

$$q-1-a = \sum_{i=0}^{f-1} (p-1-a_i)p^i,$$

which implies

$$S(a) + S(q-1-a) = \sum_{i=0}^{f-1} (p-1) = f(p-1).$$

Summing this latter expression from $a=1$ to $a=q-2$ we get

$$S(1) + S(2) + \dots + S(q-2) + S(q-2) + S(q-3) + \dots + S(1) = (q-2)f(p-1),$$

from which the Lemma follows.

□

Start with Lemma 1.5.1 to write (also use $a = [a] + \langle a \rangle$)

$$(p-1) \sum_{i=0}^{f-1} \lfloor \frac{ap^i}{q-1} \rfloor = (p-1) \sum_{i=0}^{f-1} \frac{ap^i}{q-1} - (p-1) \sum_{i=0}^{f-1} \langle \frac{ap^i}{q-1} \rangle = a - S(a). \quad (1.22)$$

For the remainder of this section let $p = 2$, so $q = 2^f$.

If $0 \leq k \in \mathcal{Z}$ write $k = rf + j$ with $0 \leq j < f$. Then $b = 2^k = 2^{rf+j} = 2^j(2^{rf} - 1) + 2^j \equiv 2^j \pmod{q-1}$. Hence for $0 \leq a \leq q-2$, $S(a + 2^k) = S(a + 2^j) =$

$$= \begin{cases} S(a) + 1 = S(a) + S(2^j) & \text{if } 2^j \notin a; \\ S(a) + S(2^j) - 1 = S(a), & \text{if } 2^j \in a \text{ but } 2^{j+1} \notin a; \\ < S(a) + S(2^j) - 1 = S(a), & \text{if } 2^j \in a \text{ and } 2^{j+1} \in a. \end{cases} \quad (1.23)$$

Lemma 1.5.4. *Using the previous lemma we can prove:*

- (i) *If $a \cap b = 2^j$ and $2^{j+1} \notin a$ or b , then $S(a + b) = S(a) + S(b) - 1$.*
- (ii) *If $a \cap b = 2^j$ and $2^{j+1} \in a$ or b , then $S(a + b) < S(a) + S(b) - 1$.*

Proof. We assume that $f > 2$, so $2^j \neq 2^{j+2}$. Suppose $a \cap b = 2^j$, and put $\bar{a} = a - 2^j$, $\bar{b} = b - 2^j$. Then by Eq. 1.23 we have the following:

$$\begin{aligned} S(a + b) &= S(\bar{a} + \bar{b} + 2^{j+1}) \\ &= \begin{cases} S(\bar{a} + \bar{b}) + 1, & \text{if } 2^{j+1} \notin \bar{a} + \bar{b}; \\ S(\bar{a} + \bar{b}), & \text{if } 2^{j+1} \in \bar{a} + \bar{b} \text{ but } 2^{j+2} \notin \bar{a} + \bar{b}; \\ < S(\bar{a} + \bar{b}), & \text{if } 2^{j+1} \in \bar{a} + \bar{b} \text{ and } 2^{j+2} \in \bar{a} + \bar{b}. \end{cases} \\ &= \begin{cases} S(a) + S(b) - 1, & \text{if } 2^{j+1} \notin a \text{ or } b; \\ S(a) + S(b) - 2, & \text{if } 2^{j+1} \in a \text{ or } b; \\ < S(a) + S(b) - 2, & \text{if } 2^{j+1} \in a \text{ or } b \text{ and } 2^{j+2} \in a \text{ or } b. \end{cases} \end{aligned}$$

□

In fact, it is easy to prove the following.

Lemma 1.5.5. *For $a = \sum_{i=0}^{f-1} a_i 2^i$, $0 \leq a_i \leq 1$ and $b = \sum_{i=0}^{f-1} b_i 2^i$, $0 \leq b_i \leq 1$, put $a \cap b = \sum_{i=0}^{f-1} c_i 2^i$, $0 \leq c_i \leq 1$, where $c_i = 1$ if and only if $a_i = b_i = 1$. Then $S(a + b) \leq S(a) + S(b) - S(a \cap b)$.*

Proof. For each $2^i \in a \cap b$, the two contributions made by 2^i in $S(a) + S(b)$ are first replaced by 2^{i+1} . There may or may not be further collapsing in $a + b$, but the value of $S(a + b)$ will be reduced by at least one in $S(a + b)$. This is true for each $2^i \in a \cap b$. \square

Theorem 1.5.6. $S(a + b) = S(a) + S(b) - 1$ if and only if $a \cap b = 2^j$ for some j with $0 \leq j \leq f - 1$, and 2^{j+1} is not in either a or b . Here $j + 1$ is taken modulo f to satisfy $0 \leq j + 1 \leq f - 1$.

Proof. This is an immediate corollary of Lemma 1.5.4 and Lemma 1.5.5. \square

Lemma 1.5.7. For $1 < k < f$ with $(k, f) = (k - 1, f - 1) = 1$ let $B_k(f)$ be the number of a 's, $0 < a < 2^f - 1$ for which

$$S(a) + S((k - 1)a) = S(ka) + 1. \quad (1.24)$$

Then $B_k(f)$ is a multiple of f and we may put $A_k(f) = B_k(f)/f$.

Proof. With $p = 2$ in Eq. 1.22 we have

$$\begin{aligned} & \sum_{i=0}^{f-1} \left\{ \left\lfloor \frac{ak2^i}{q-1} \right\rfloor - \left\lfloor \frac{a2^i}{q-1} \right\rfloor - \left\lfloor \frac{a(k-1)2^i}{q-1} \right\rfloor \right\} = \\ & = \{ak - S(ak)\} - \{a - S(a)\} - \{a(k-1) - S(a(k-1))\} \\ & = S(a) + S(a(k-1)) - S(ak). \end{aligned} \quad (1.25)$$

Since the binary representation of $2a$ modulo $q - 1$ is obtained by simply rotating the binary representation of a modulo $q - 1$ by “one step”, i.e., all the digits are moved one step to the left, with a 1 that would be moved beyond the leftmost place moved (“rotated”) to the rightmost place. So, as we saw earlier, $S(a) = S(2a)$. Hence given any solution a to Eq. 1.24, $a2^i$ is also a solution for $0 \leq i \leq f - 1$. Moreover, we claim that $a \cdot 2^j$, $0 \leq j \leq f - 1$, are necessarily *distinct* modulo $2^f - 1$. For if $a2^i \equiv a2^j \pmod{q-1}$ for $0 \leq i < j \leq f - 1$, and if a is a solution to $S(a) + S((k - 1)a) = S(ka) + 1$, then the sum over i in Eq. 1.25 would have more than one term equal to 1 (and all terms are nonnegative because in general $\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor$), contradicting the choice of a . (For if $a2^i \equiv a2^j \pmod{q-1}$, then also $ak2^i \equiv ak2^j \pmod{q-1}$, etc.) \square

We now give one application of Theorem 1.5.6 to the special case where f is odd and $b = 5a$. Hence if $k = 6$, then $(k, q - 1) = (k - 1, q - 1) = 1$ and the goal is to determine all a modulo $q - 1$ for which

$$S(a) + S(5a) = S(6a) + 1. \quad (1.26)$$

Theorem 1.5.8. *Let f be an odd integer ≥ 3 . The binary representations of all the solutions $a \pmod{q - 1}$ to the equation*

$$S(a) + S(5a) = S(6a) + 1$$

can be constructed by the following procedure:

Step 1. Form all the possible binary strings of length at most f by concatenating blocks of the form 01, 0011, 00111, subject to the following constraints:

(A) In a string of length less than f , the rightmost block must be 01, and the block 00111 must not occur.

(B) In a string of length f , the block 00111 occurs exactly once, namely, as the rightmost block.

Step 2. Given a string of length k obtained through Step 1, append $(f - k)$ 0's on the left to form a string of length f .

Step 3. All binary representations of all solutions a modulo $q - 1$ to Eq. 1.25 are obtained by forming all possible rotations of the strings that were constructed in Step 2.

N.B. In an appendix we have included the treatment written up by Carey Jenkins proving this result.

Write $A_6(f) = B_6(f)/f$, where $B_6(f)$ is the number of solutions mod $q - 1 = 2^f - 1$ to Eq. 1.26. We are interested here in the case where f is odd, say $f = 2m + 1$. So put $a_n = A_6(2n + 1)$. We know $a_1 = A_6(3) = 1$, $a_2 = A_6(5) = 3$.

Theorem 1.5.9. *If F_n is the n th Fibonacci number, then $a_n = A_6(2n + 1) = 2F_n - 1$.*

Proof. We start by showing that

$$A_6(f) = A_6(f - 2) + A_6(f - 4) + 1. \quad (1.27)$$

The recurrence is to be viewed as a recurrence for the number $B_6(f)/f$ of strings constructed in Step 1 of Theorem 1.5.8, i.e., before appending the

spare 0's and rotating the obtained strings of length f . There are $B_6(f)/f$ such strings, since due to the particular form of the strings, all the f rotations in Step 3 are indeed different from each other.

For given f , the strings that are constructed in Step 1 can be separated into three sets: first, there is the string 01 of length 2; then there is the set of strings of length greater than 2 with leftmost block 01, and finally there is the set of strings with leftmost block 0011. The first string contributes the 1. The second set of strings can be obtained by performing Step 1 with f replaced by $f - 2$ and then appending 01 to the left of each of the obtained strings. The third set of strings can be obtained by first performing Step 1 with f replaced by $f - 4$ and then appending 0011 to the left of each of the obtained strings. Summing over the three types of sets of strings we obtain the recurrence of Eq. 1.5.8. Interpret the recurrence for the a_i to get:

$$a_{n+2} = a_{n+1} + a_n + 1. \quad (1.28)$$

Also, since $a_{n+1} = a_n + a_{n-1} + 1$, solving for a_0 we find $a_0 = 1$.

Now put $A(x) = \sum_{n=0}^{\infty} a_n x^n$ and multiply both sides by x^{n+2} and sum from $n = 0$ to $n = \infty$:

$$\sum_{n=0}^{\infty} a_{n+2} x^{n+2} = \sum_{n=0}^{\infty} a_{n+1} x^{n+2} + \sum_{n=0}^{\infty} a_n x^{n+2} + \sum_{n=0}^{\infty} x^{n+2}.$$

After rewriting this and collecting terms we obtain:

$$A(x) = \frac{1 - x + x^2}{(1 - x - x^2)(1 - x)} = \frac{-1}{1 - x} + \frac{2}{1 - x - x^2} = \sum_{n=0}^{\infty} (2F_n - 1)x^n,$$

which says that $a_n = 2F_n - 1$, where F_n is the n th Fibonacci number, $F_0 = F_1 = 1$. (This requires knowing that $1/(1 - x - x^2)$ is the ordinary generating function for the Fibonacci sequence.)

□

1.6 Hyperovals

In this section we review briefly the basic facts about hyperovals in finite desarguesian projective planes. For a more thorough treatment with proofs

see the notes “Topics in Finite Geometry: Ovals, Ovoids and Generalized Quadrangles” by S. E. P. A k -arc in the projective plane $PG(2, q)$, with q a prime power, is a set of k points, no three of which are collinear. The maximum value of k is $q + 1$ or $q + 2$, according as q is odd or even. If $k = q + 1$ a k -arc is called an *oval*. If q is even, a $q + 2$ -arc is called a *hyperoval*. If q is even each oval is contained in a unique hyperoval. A celebrated theorem of B. Segre says that when q is odd, each oval is actually a conic, i.e., the set of points whose coordinates satisfies an irreducible quadratic equation. The classic example of a hyperoval when q is even is a conic together with its nucleus.

Two hyperovals are said to be *projectively equivalent* if one hyperoval can be transformed into the other by a projective linear transformation (an *homography*), i.e., by an element of $PGL(3, q)$. By the Fundamental Theorem of Projective Geometry, the group $PGL(3, q)$ of homographies of $PG(2, q)$ is sharply transitive on ordered quadrangles. Thus every hyperoval can be mapped by an homography to a hyperoval containing the *fundamental quadrangle* $(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)$. From now on we will restrict our attention to those hyperovals in $PG(2, q)$ with q even and greater than 2 which contain the fundamental quadrangle. The following result of Segre shows that any such hyperoval can be expressed in terms of a *permutation polynomial* over F_q , i.e., a polynomial which when interpreted as a function permutes F_q .

Theorem 1.6.1. (Segre). *Let $q > 2$ be a power of 2. Then any hyperoval in $PG(2, q)$ containing the fundamental quadrangle is equal to a $(q + 2)$ -arc*

$$D(f) = \{(1, t, f(t)) : t \in F_q\} \cup \{(0, 1, 0), (0, 0, 1)\},$$

where f is a permutation polynomial over F_q of degree at most $q - 2$, satisfying $f(0) = 0$, $f(1) = 1$, and such that for each $s \in F_q$,

$$f_s(x) = \begin{cases} \frac{f(x+s)+f(s)}{x}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0, \end{cases}$$

is a permutation polynomial.

Conversely, every such set $D(f)$ is an hyperoval.

Polynomials $f(x)$ as described in Theorem 1.6.1 are called *o-polynomials*.

The hyperovals of interest in these notes are the *monomial hyperovals*. These are hyperovals in $PG(2, q)$ (with $q = 2^d$) projectively equivalent to a

hyperoval

$$D(x^k) = \{(1, t, t^k) : t \in F_q\} \cup \{(0, 1, 0), (0, 0, 1)\}.$$

It is well known that if $D(x^k)$ is an hyperoval, then $(k, q-1) = (k-1, q-1) = 1$. Moreover, given k for which $(k, q-1) = (k-1, q-1) = 1$, then $D(x^j)$ is an hyperoval projectively equivalent to $D(x^k)$ if and only if j is congruent modulo $q-1$ to an element of $\{k, 1/k, 1-k, 1/(1-k), k/(k-1), (k-1)/k\}$.

The known examples of monomial hyperovals are as follows:

Ex. 1. The *regular* hyperoval $D(x^2)$ (conic plus nucleus);

Ex. 2. The *translation* hyperovals $D(x^{2^i})$ where $(d, i) = 1$.

Ex. 3. The *Segre* hyperoval $D(x^6)$, where d is odd.

Ex. 4. The *Glynn Type (I)* hyperovals $D(x^{\sigma+\gamma})$, where $\sigma^2 = 2$ and $\gamma^2 = \sigma$, i.e., $\sigma = 2^{(d+1)/2}$, and $\gamma = 2^{(3d+1)/4}$ if $d \equiv 1 \pmod{4}$, $\gamma = 2^{(d+1)/4}$ if $d \equiv 3 \pmod{4}$.

Ex. 5. The *Glynn type (II)* hyperovals $D(x^{3\sigma+4})$, where σ is as above.

For small values of q there is some overlap among these classes, but for $q > 32$ they are distinct except that the regular hyperoval is always a translation hyperoval.

Lemma 1.6.2. *Let $q = 2^d$. The $(q+2)$ -set $D(x^k) = \{(1, t, t^k) : t \in F_q\} \cup \{(0, 1, 0), (0, 0, 1)\}$ in $PG(2, q)$ is a hyperoval if and only if $(k, q-1) = 1$ and $\tau : F_q \rightarrow F_q : x \mapsto x^k + x$ is a two-to-one map.*

Proof. It is clear that $D(x^k)$ is an hyperoval if and only if each line meets it in exactly 0 or two points. For $a \neq 0$ the line $[a, 0, 0]^T = \langle (0, 1, 0), (0, 0, 1) \rangle$ meets $D(x^k)$ in exactly two points. The line $[a, 1, 0]^T$ contains $(0, 0, 1)$ but not $(0, 1, 0)$, and contains $(1, t, t^k)$ if and only if $t = a$, so meets $D(x^k)$ in exactly two points. The line $[a, 0, 1]^T$ contains the point $(0, 1, 0)$ but not $(0, 0, 1)$ and contains $(1, t, t^k)$ if and only if $f(t) = 1$, so meets $D(x^k)$ in exactly two points if and only if $(k, q-1) = 1$. Finally, $[a, b, c]^T$ with $bc \neq 0$ does not contain either $(0, 1, 0)$ or $(0, 0, 1)$ and meets $D(x^k)$ in exactly 0 or two points if and only if $a + bt + ct^k = 0$ has 0 or two solutions. Divide by c and replace t with $(\frac{b}{c})^{\frac{1}{k-1}} \cdot s$ to see that $[a, b, c]^T$ meets $D(x^k)$ in exactly 0 or two points if and only if the map $x \mapsto x^k + x$ is two-to-one. \square

Eventually we will use monomial hyperovals to produce cyclic difference sets, a construction first given by Maschietti.

1.7 The Transfer Matrix Method

In this section we give an introduction to the Transfer Matrix Method. The actual application made in [EHKX99] is somewhat different from the material presented here and can probably be understood without reading this section, but we wanted to include in these notes a general introduction to this method. (See Math 6409 notes for more on this subject.)

The Transfer Matrix Method, when applicable, is often used to show that a given sequence has a rational generating function. Sometimes that knowledge helps one to compute the generating function using other information.

Let A be a $p \times p$ matrix over the complex numbers \mathcal{C} . Let $f(\lambda) = \det(\lambda I - A) = a_{p-n_0}\lambda^{n_0} + \cdots + a_1\lambda^{p-1} + \lambda^p$ be the characteristic polynomial of A with $a_{p-n_0} \neq 0$. So the reverse polynomial \hat{f} is given by $\hat{f}(\lambda) = 1 + a_1\lambda + \cdots + a_{p-n_0}\lambda^{p-n_0}$. Hence $\det(I - \lambda A) = \lambda^p \det(\frac{1}{\lambda}I - A) = \hat{f}(\lambda)$. We have essentially proved the following:

Lemma 1.7.1. *If $f(\lambda) = \det(\lambda I - A)$, then $\hat{f}(\lambda) = \det(I - \lambda A)$. Moreover, if A is invertible, so $n_0 = 0$, then $\hat{f} = f$, and $f(\lambda) = \det(\lambda I - A)$ iff $\hat{f}(\lambda) = \det(I - \lambda A)$.*

For $1 \leq i, j \leq p$, define the generating function

$$F_{ij}(A, \lambda) = \sum_{n \geq 0} (A^n)_{ij} \lambda^n. \quad (1.29)$$

Here $A^0 = I$ even if A is not invertible.

Theorem 1.7.2. $F_{ij}(A, \lambda) = \frac{(-1)^{i+j} \det[(I - \lambda A) : j, i]}{\det(I - \lambda A)}$.

Proof. Here $(B : i, j)$ denotes the matrix obtained from B by deleting the i^{th} row and the j^{th} column. Recall that $(B^{-1})_{ij} = \frac{(-1)^{i+j} \det(B : j, i)}{\det(B)}$. Suppose that $B = I - \lambda A$, so $B^{-1} = (I - \lambda A)^{-1} = \sum_{n=0}^{\infty} A^n \lambda^n$, and $\frac{(-1)^{i+j} \det(B : j, i)}{\det(B)} = (B^{-1})_{ij} = \sum_{n=0}^{\infty} (A^n)_{ij} \lambda^n = F_{ij}(A, \lambda)$, proving the theorem. \square

Corollary 1.7.3. F_{ij} is a rational function of λ whose degree is strictly less than the multiplicity n_0 of 0 as an eigenvalue of A .

Proof. Let $f(\lambda) = \det(\lambda I - A)$, so $\hat{f}(\lambda) = \det(I - \lambda A)$ has degree $p - n_0$, and $\deg(\det(I - \lambda A) : j, i) \leq p - 1$. Hence $\deg(F_{ij}(A, \lambda)) \leq (p - 1) - (p - n_0) = n_0 - 1 < n_0$. \square

Now write $q(\lambda) = \det(I - \lambda A) = \hat{f}(\lambda)$. If w_1, \dots, w_q are the nonzero eigenvalues of A , then $\frac{1}{w_1}, \dots, \frac{1}{w_q}$ are the zeros of $q(\lambda)$, so

$$q(\lambda) = a \left(\lambda - \frac{1}{w_1} \right) \cdots \left(\lambda - \frac{1}{w_q} \right)$$

for some nonzero a . From the definition of $q(\lambda)$ we see that $q(0) = \det(I) = 1$, so

$$q(\lambda) = (-1)^q w_1 \cdots w_q \left(\lambda - \frac{1}{w_1} \right) \cdots \left(\lambda - \frac{1}{w_q} \right). \quad (1.30)$$

Then after computing the derivative $q'(\lambda)$ we see easily that

$$\begin{aligned} \frac{-\lambda q'(\lambda)}{q(\lambda)} &= -\lambda \left\{ \frac{1}{\lambda - \frac{1}{w_1}} + \cdots + \frac{1}{\lambda - \frac{1}{w_q}} \right\} \\ &= \frac{w_1 \lambda}{1 - w_1 \lambda} + \frac{w_2 \lambda}{1 - w_2 \lambda} + \cdots + \frac{w_q \lambda}{1 - w_q \lambda} \\ &= \sum_{i=1}^q \sum_{n=1}^{\infty} w_i^n \lambda^n = \sum_{n=1}^{\infty} \left(\sum_{i=1}^q w_i^n \right) \lambda^n = \sum_{n=1}^{\infty} \text{tr}(A^n) \lambda^n. \end{aligned} \quad (1.31)$$

We have proved the following corollary:

Corollary 1.7.4. *If $q(\lambda) = \det(I - \lambda A)$, then $\sum_{n=1}^{\infty} \text{tr}(A^n) \lambda^n = \frac{-\lambda q'(\lambda)}{q(\lambda)}$.*

Let $D = (V, E, \phi)$ be a finite digraph, where $V = \{v_1, \dots, v_p\}$ is the set of vertices, E is a set of (directed) edges or arcs, and $\phi : E \rightarrow V \times V$ determines the edges. If $\phi(e) = (u, v)$, then e is an edge from u to v , with initial vertex $\text{int}(e) = u$ and final vertex $\text{fin}(e) = v$. If $u = v$, then e is a *loop*. A *walk* Γ in D of length n from u to v is a sequence $e_1 e_2 \cdots e_n$ of n edges such that $\text{int}(e_1) = u$, $\text{fin}(e_n) = v$, and $\text{fin}(e_i) = \text{int}(e_{i+1})$ for $1 \leq i < n$. If also $u = v$, then Γ is called a *closed walk based at u* . (Note: If Γ is a closed walk, then $e_i e_{i+1} \cdots e_n e_1 \cdots e_{i-1}$ is in general a different closed walk.)

Now let $w : E \rightarrow R$ be a weight function on E (R is some commutative ring; usually $R = \mathcal{C}$ or $R = \mathcal{C}[x]$.) If $\Gamma = e_1 e_2 \cdots e_n$ is a walk, then the *weight* of Γ is defined by $w(\Gamma) = w(e_1) w(e_2) \cdots w(e_n)$. Fix i and j , $1 \leq i, j \leq p$. Put $A_{ij}(n) = \sum_{\Gamma} w(\Gamma)$, where the sum is over all walks Γ in D of length n from v_i to v_j . In particular, $A_{ij}(0) = \delta_{ij}$. The fundamental problem treated

by the transfer matrix method (TMM) is the evaluation of $A_{ij}(n)$, or at least the determination of some generating function for the $A_{ij}(n)$.

Define a $p \times p$ matrix $A = (A_{ij})$ by

$$A_{ij} = \sum_e w(e),$$

where the sum is over all edges with $\text{int}(e) = v_i$ and $\text{fin}(e) = v_j$. So $A_{ij} = A_{ij}(1)$. A is the *adjacency matrix of D with respect to the weight function w* .

Theorem 1.7.5. *Let $n \in \mathcal{N}$. Then the (i, j) -entry of A^n is equal to $A_{ij}(n)$. (By convention, $A^0 = I$ even if A is not invertible.)*

Proof. $(A^n)_{ij} = \sum A_{i i_1} A_{i_1 i_2} \cdots A_{i_{n-1} j}$, where the sum is over all sequences $(i_1, \dots, i_{n-1}) \in [p]^{n-1}$. (Here $i = i_0$ and $j = i_n$.) The summand is zero unless there is a walk $e_1 \cdots e_n$ from v_i to v_j with $\text{int}(e_k) = v_{i_{k-1}}$ ($1 \leq k \leq n$), and $\text{fin}(e_k) = v_{i_k}$ ($1 \leq k \leq n$). If such a walk exists, then the summand is equal to the sum of the weights of all such walks. \square

We give a special case that occasionally works out in a very satisfying way. Let $C_D(n) = \sum_{\Gamma} w(\Gamma)$, where the sum is over all *closed* walks Γ in D of length n . In this case we have the following.

Corollary 1.7.6. $\sum_{n \geq 1} C_D(n) \lambda^n = \frac{-\lambda q'(\lambda)}{q(\lambda)}$, where $q(\lambda) = \det(I - \lambda A)$.

Proof. Clearly $C_D(1) = \text{tr}(A)$, and by Theorem 1.7.5 we have $C_D(n) = \text{tr}(A^n)$. Hence by Cor 1.7.4 we have $\sum_{n \geq 1} C_D(n) \lambda^n = \frac{-\lambda q'(\lambda)}{q(\lambda)}$. \square

Often an enumeration problem can be represented as counting the number of sequences $a_1 a_2 \cdots a_n \in [p]^n$ of integers $1, \dots, p$ subject to certain restrictions on the subsequences $a_i a_{i+1}$ that may appear. In this case we form a digraph D with vertices $v_i = i$, $1 \leq i \leq p$, and put an arc $e = (i, j)$ from i to j provided the subsequence ij is permitted. So a permitted sequence $a_{i_1} a_{i_2} \cdots a_{i_n}$ corresponds to a walk $\Gamma = (i_1, i_2)(i_2, i_3) \cdots (i_{n-1}, i_n)$ in D of length $n - 1$ from i_1 to i_n . If $w(e) = 1$ for all edges in D and if A is the adjacency matrix of D with respect to this particular weight function, then clearly $f(n) := \sum_{i, j=1}^p A_{ij}(n-1)$ is the number of sequences $a_1 a_2 \cdots a_n \in [p]^n$

subject to the restrictions used in defining D . Put $q(\lambda) = \det(I - \lambda A)$ and $q_{ij}(\lambda) = \det((I - \lambda A) : j, i)$. Then by Theorem 1.7.2

$$\begin{aligned} F(\lambda) &:= \sum_{n \geq 0} f(n+1)\lambda^n = \sum_{n \geq 0} \left(\sum_{i,j=1}^p A_{ij}(n) \right) \lambda^n \\ &= \sum_{i,j=1}^p \sum_{n \geq 0} A_{ij}(n)\lambda^n = \sum_{i,j=1}^p F_{ij}(A, \lambda) = \sum_{i,j=1}^p \frac{(-1)^{i+j} q_{ij}(\lambda)}{q(\lambda)}. \end{aligned} \quad (1.32)$$

We state this as a corollary.

Corollary 1.7.7. *If $w(e) = 1$ for all edges in D and $f(n)$ is the number of sequences $a_1 a_2 \cdots a_n \in [p]^n$ subject to the restrictions used in defining D , then*

$$\sum_{n \geq 0} f(n+1)\lambda^n = \sum_{i,j=1}^p \frac{(-1)^{i+j} q_{ij}(\lambda)}{q(\lambda)}. \quad (1.33)$$

1.8 Linear Recurrences

In treating the Glynn hyperovals we will make use of the result (possibly folklore) that when it is known (by some abstract means) that a sequence satisfies *some* linear recurrence, and when a bound for the order of the recurrence is also known, then one needs only to check a certain number of special instances of a *specific* recurrence to prove that the sequence satisfies this recurrence “always.” The precise statement is given in the following theorem.

Theorem 1.8.1. *Let $(f_n)_{n \geq 0}$ be a sequence of complex numbers. Suppose that we know that the ordinary generating function $\sum_{n \geq 0} f_n z^n$ for the sequence is rational, i.e., that it equals $p(z)/q(z)$, where $p(z)$ and $q(z)$ are polynomials in z , and that the degree of the numerator $p(z)$ is at most P , and the degree of the denominator $q(z)$ is at most Q . If the sequence (f_n) satisfies the recurrence*

$$\sum_{i=0}^k a_i f_{n-i} = c \quad (1.34)$$

for $n = n_0, \dots, N$, where $n_0 \geq k$, $N = \max \{P + k + 1, Q + n_0\}$, and where a_0, a_1, \dots, a_k and c are some given complex numbers, then the recurrence of 1.33 is satisfied for all $n \geq n_0$.

Proof. Put $a(z) = \sum_{i=0}^k a_i z^i$, $F(z) = \sum_{i=0}^{\infty} f_i z^i$. Then

$$\begin{aligned} a(z)F(z) &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^k a_i f_{n-i} \right) z^n = \\ &= \sum_{n=0}^{n_0-1} r_n z^n + \sum_{n=n_0}^N \left(\sum_{i=0}^k a_i f_{n-i} \right) z^n + \sum_{n=N+1}^{\infty} \left(\sum_{i=0}^k a_i f_{n-i} \right) z^n = \\ &= r(z) + \sum_{n=n_0}^N c \cdot z^n + \sum_{n=N+1}^{\infty} c z^n + \sum_{n=N+1}^{\infty} \left(\left(\sum_{i=0}^k a_i f_{n-i} \right) - c \right) z^n = \\ &= r(z) + \frac{c}{1-z} + z^{N+1} \cdot S(z), \text{ where } S(z) \text{ vanishes iff Eq. 1.33 holds} \\ &\quad \text{for all } n \geq n_0. \end{aligned}$$

Multiply this last equation by $(1-z)q(z)$:

$$(1-z)a(z)p(z) = (1-z)q(z)r(z) + c \cdot q(z) + z^{N+1}(1-z)q(z)S(z).$$

The left hand side has degree less than or equal to $1+k+P \leq N$. The first term on the right hand side has degree less than or equal to $1+Q+(n_0-1) = Q+n_0 \leq N$. Similarly, the second term of the right hand side has degree less than or equal to $Q \leq N$. Clearly the last term on the right hand side has degree greater than N if it is nonzero. It follows that $S(z) = 0$. \square

1.9 Multiplier Theory

Strictly speaking, we do not need the theory of multipliers of abelian difference sets in order to reach our goal of using Stickelberger's theorem to evaluate the p -ranks of the designs arising from the Segre ovals. On the other hand, we feel that any introduction to difference sets should include the basic results on multipliers. Hence we have included this section as a kind of appendix to Chapter 1.

Throughout this section we assume that G is an abelian group of order v written multiplicatively. Also, k and λ are integers satisfying $0 < \lambda < k$ and $\lambda(v-1) = k(k-1)$, and we write $n = k - \lambda$. Then D is a k -subset of G that is a (v, k, λ) -quotient set in G , i.e., in $\mathcal{Z}[G]$ we have

$$DD^{-1} = n + \lambda G. \quad (1.35)$$

For any integer t , the map $\lambda_t : g \mapsto g^t$ is an endomorphism of G and induces an endomorphism of $\mathcal{Z}[G]$ also denoted λ_t :

$$\lambda_t : \mathcal{Z}[G] \rightarrow \mathcal{Z}[G] : \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g^t.$$

For $A, B \in \mathcal{Z}$ and $m \in \mathcal{Z}$, we say $A \equiv B \pmod{m}$ provided $A - B = mC$ for some $C \in \mathcal{Z}[G]$.

This leads to an elementary but useful lemma.

Lemma 1.9.1. *Let p be a prime and $A = \sum_{g \in G} a_g g \in \mathcal{Z}[G]$. Then*

$$A^p \equiv \lambda_p(A) \pmod{p}.$$

Proof. We proceed by induction on the number of nonzero coefficients of $A \in \mathcal{Z}[G]$. First suppose A has one nonzero term, say $A = ag$, $a \in \mathcal{Z}$, $g \in G$. Then $A^p = (ag)^p = a^p g^p \equiv a g^p = \lambda_p(A) \pmod{p}$.

Recall that if $1 \leq i \leq p-1$, then $\binom{p}{i} \equiv 0 \pmod{p}$. So suppose that H is some subset of G for which $B = \sum_{g \in H} b_g g$ satisfies $B^p \equiv \lambda_p(B) \pmod{p}$. Then if $A = b_h h + B$ for some $h \in G \setminus H$, we have

$$A^p = (b_h h + B)^p \equiv (b_h h)^p + B^p \equiv b_h h^p + \lambda_p(B) = \lambda_p(A).$$

□

Let G be a multiplicatively written abelian group and let D be a quotient set in G . An automorphism α of G is said to be a *multiplier* of D if and only if the quotient set $\alpha(D)$ is a translate (i.e., *coset*) of D , that is if and only if $\alpha(D) = Dg = \{dg : d \in D\}$ for some $g \in G$. For example, the automorphism $a \mapsto a^3$ of the cyclic group $C_{13} = \langle g \rangle$ is a multiplier of the $(13, 4, 1)$ quotient set $\{g^0, g^2, g^3, g^7\}$ since $\{g^0, g^6, g^9, g^8\} = \{g^0, g^2, g^3, g^7\}g^6$.

More generally, if t is any integer relatively prime to the order of G , and hence to the exponent of G (the least common multiple of the orders of the elements of G), then $\lambda_t : g \mapsto g^t$ is an automorphism of G . If λ_t is a

multiplier of a quotient set D of G , we say that λ_t is a *numerical multiplier* or *Hall multiplier* of D .

Note: An automorphism α of G is a multiplier of a quotient set D in G if and only if in the group ring $\mathcal{Z}[G]$, $\alpha(D) = Dg$ for some $g \in G$.

It will be convenient to write automorphisms as exponents. So instead of writing $\alpha(D)$ from now on, for example, we will write $D^\alpha = \{d^\alpha : d \in D\}$. Moreover, for some $A \in \mathcal{Z}[G]$, instead of writing A^{λ_t} we will just write A^t . So in particular $D^{-1} = \sum_{d \in D} d^{-1}$.

Lemma 1.9.2. *Let α be an automorphism of G and let D be a (v, k, λ) -quotient set in G . Consider*

$$S := D^\alpha D^{-1} - \lambda G.$$

Then α is a multiplier of D if and only if S has nonnegative coefficients.

Proof. If α is a multiplier of D , then $D^\alpha = gD$ for some $g \in G$, so that

$$D^\alpha D^{-1} = gDD^{-1} = g(n + \lambda G) = ng + \lambda G.$$

So in this case S , as defined above, is equal to ng for some $g \in G$, where $n = k - \lambda$, as usual. In particular, it has nonnegative coefficients. Note that, conversely, if $D^\alpha D^{-1} = ng + \lambda G$, we can multiply this by D to find

$$D^\alpha DD^{-1} = D^\alpha \cdot (n + \lambda G) = n \cdot D^\alpha + \lambda DG = n \cdot D^\alpha + \lambda kG,$$

and also that

$$(D^\alpha D^{-1})D = (ng + \lambda G)D = ng \cdot D + \lambda kG.$$

Hence $D^\alpha = gD$, implying that α is a multiplier.

Since α is an automorphism of G , the map $\alpha : \mathcal{Z}[G] \rightarrow \mathcal{Z}[G] : \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g^\alpha$ is an automorphism. Hence $D^\alpha D^{-\alpha} = n + \lambda G$, i.e., D^α is also a quotient set, and

$$\begin{aligned} SS^{-1} &= \{D^\alpha D^{-1} - \lambda G\} \{D^{-\alpha} D - \lambda G\} \\ &= \{n + \lambda G\}^2 - 2\lambda k^2 G + \lambda^2 v G \\ &= n^2 + 2\lambda(n + \lambda v - k^2)G = n^2 s \\ &= n^2. \end{aligned}$$

Suppose that $S = \sum_{g \in G} s_g g$ with nonnegative coefficients s_g . If $s_g > 0$ and $s_h > 0$ for $g, h \in G$, then the coefficient of gh^{-1} in $SS^{-1} = n^2$ is at least $s_g s_h$, i.e., strictly positive. Hence gh^{-1} must be the identity e of G , i.e., $g = h$. So S can have only one positive coefficient, say $S = s_g g$. The equation $SS^{-1} = n^2$ forces $s_g = n$ and we have shown that $S = ng$. As noted above, we may conclude that α is a multiplier. \square

We are now ready for the famous multiplier theorem. (This version is a generalization by Hall and Ryser of the original theorem first proved by M. Hall, Jr.)

We emphasize that for a prime p , $(D)^p$ denotes $(\sum_{d \in D} d)^p$, whereas D^p denotes $\sum_{d \in D} d^p$. Lemma 1.9.1 says that these two expressions are congruent modulo p .

Theorem 1.9.3. *Let D be a (v, k, λ) -quotient set in an abelian group G of order v . Let p be a prime dividing n with $(p, v) = 1$ and $p > \lambda$. Then p is a Hall multiplier of D .*

Proof. Let $S = D^p D^{-1} - \lambda G$. By Lemma 1.9.2 it will suffice to show that S has nonnegative coefficients. By Lemma 1.9.1 we have

$$\begin{aligned} D^p D^{-1} &\equiv (D)^p D^{-1} \equiv (D)^{p-1} D D^{-1} \\ &\equiv (D)^{p-1} \cdot (n + \lambda G) \equiv n(D)^{p-1} + \lambda k^{p-1} G \\ &\equiv \lambda G \pmod{p}, \end{aligned}$$

since p divides n and $k^{p-1} \equiv 1 \pmod{p}$. Thus the coefficients of $D^p D^{-1}$, which are clearly nonnegative, are all congruent to λ modulo p . Since $p > \lambda$, it must be that the coefficients of $D^p D^{-1}$ are greater than or equal to λ , i.e., S has nonnegative coefficients. \square

Chapter 2

Algebraic Number Theory

In this chapter we give the beginning of the theory of algebraic numbers. Our primary interest is in the fact that the ring D of algebraic integers in some finite extension $Q(\theta)$ of the rationals is a Dedekind domain, especially in how a prime ideal of \mathcal{Z} generates an ideal \mathcal{P} in D and how \mathcal{P} factors into a product of powers of prime ideals of D . We present just enough of this theory to make the following chapter on Cyclotomic extensions intelligible. We assume that the reader already knows some field theory including a bit of Galois theory.

2.1 Discriminants of Number Fields

An *algebraic number field* is a finite extension K of the rational field Q , say $K = Q(\theta)$. Let $f(x)$ be the minimal polynomial for θ over Q , say $\deg f(x) = n$. Then in C , $f(x)$ has exactly n distinct roots (say $\theta = \theta_1$):

$$f(x) = \prod_{i=1}^n (x - \theta_i).$$

The roots $\theta = \theta_1, \theta_2, \dots, \theta_n$ are called the *conjugates* of θ over Q . It follows that $f(x)$ is also the minimal polynomial for each of the conjugates of θ over Q . Moreover, there is a unique field isomorphism $\sigma_i : Q(\theta) \rightarrow Q(\theta_i) : \theta \mapsto \theta_i$. If $\alpha \in Q(\theta)$, then $\alpha = r(\theta)$ for a unique $r \in Q[x]$ with degree less than n , and then

$$\sigma_i(\alpha) = r(\theta_i).$$

Conversely, If $\sigma : K \rightarrow C$ is a monomorphism, then σ is the identity on Q , and $0 = \sigma(f(\theta)) = f(\sigma(\theta))$, so that $\sigma(\theta)$ is one of the θ_i , and hence σ is one of the σ_i .

For each $\alpha \in K = Q(\theta)$, if $\alpha = r(\theta)$ for $r(x) \in Q[x]$, then define the *field polynomial of α over K* to be

$$f_\alpha(x) = \prod_i (x - r(\theta_i))$$

where the θ_i run through all zeros of the minimum polynomial f of θ , whose coefficients are in Q . It is easy to see that the coefficients of $f_\alpha(x)$ are of the form

$$h(\theta_1, \dots, \theta_n)$$

where $h(x_1, \dots, x_n)$ is a symmetric polynomial in $Q[x_1, \dots, x_n]$. It follows that the coefficients of $f_\alpha(x)$ are in Q , i.e.,

Theorem 2.1.1. *For each $\alpha \in K = Q(\theta)$, $f_\alpha(x) \in Q[x]$.*

The elements $\sigma_i(\alpha)$, for $1 \leq i \leq n$, are called the *K -conjugates* of α . Although the θ_i are distinct (and are the K -conjugates of θ), it is not always the case that the K -conjugates of α are distinct: for example, $\sigma_i(1) = 1$ for all i . The general situation is described in the next theorem.

Theorem 2.1.2. *With the above notation:*

- (a) *The field polynomial f_α is a power of the minimum polynomial p_α ;*
- (b) *The K -conjugates of α are the zeros of p_α in C , each repeated n/m times, where the degree m of p_α is a divisor of n ;*
- (c) *The element α is in Q if and only if all of its K -conjugates are equal;*
- (d) *$Q(\alpha) = Q(\theta)$ if and only if all K -conjugates of α are distinct.*

Proof. The minimum polynomial p_α is irreducible, and α is a zero of f_α , so that $f_\alpha = p_\alpha^s h$ where p_α and h are coprime and both are monic. We claim that h is constant. If not, some $\alpha_i = \sigma_i(\alpha) = r(\theta_i)$ is a zero of h , where $\alpha = r(\theta)$. Hence if $g(x) = h(r(x))$ then $g(\theta_i) = 0$. Let p be the minimum polynomial of θ over Q , and hence also of each θ_i . Then p divides g , so that $g(\theta_j) = 0$ for all j , and in particular $g(\theta) = 0$. Therefore, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$. This forces p_α to divide h , which is a contradiction. Hence h is a constant and monic, so $h = 1$ and $f = (p_\alpha)^s$, proving (a).

(b) is an immediate consequence of (a).

To prove (c), it is clear that $\alpha \in Q$ implies $\sigma_i(\alpha) = \alpha \in Q$. Conversely, if all $\sigma_i(\alpha)$ are equal, then since the zeros of p_α are distinct and $f_\alpha = (p_\alpha)^s$, then the degree of p_α must be 1, forcing $\alpha \in Q$.

Finally, for (d): if all $\sigma_i(\alpha)$ are distinct, then the degree of p_α must equal n , and hence $[Q(\alpha) : Q] = n = [Q(\theta) : Q]$. This implies that $Q(\alpha) = Q(\theta)$. Conversely, if $Q(\alpha) = Q(\theta)$, then the degree of p_α is n , implying that the $\sigma_i(\alpha)$ are distinct. \square

Still with $K = Q(\theta)$ of degree n over Q , let $\{\alpha_1, \dots, \alpha_n\}$ be a Q -basis for K . We define the *discriminant* of this basis to be

$$\begin{aligned} \Delta[\alpha_1, \dots, \alpha_n] &:= (\det[\sigma_i(\alpha_j)])^2 = \\ &= \det \left[\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \right] \\ &= \det (\text{Tr}(\alpha_i \alpha_j)), \end{aligned}$$

where $\text{Tr}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$.

If $\{\beta_1, \dots, \beta_n\}$ is another Q -basis of K , then for $1 \leq k \leq n$ there are $c_{ik} \in Q$ such that

$$\beta_k = \sum_{i=1}^n c_{ik} \alpha_i \text{ and } \det(c_{ik}) \neq 0.$$

So

$$(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n) \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}.$$

This leads to the following:

$$\begin{aligned}
\Delta[\beta_1, \dots, \beta_n] &= (\det[\sigma_i(\beta_k)])^2 \\
&= \left(\det[\sigma_i(\sum_j c_{jk}\alpha_j)] \right)^2 \\
&= \left(\det \left[\sum_j c_{jk}\sigma_i(\alpha_j) \right] \right)^2 \\
&= \left(\det \left[\sum_j \sigma_i(\alpha_j)c_{jk} \right] \right)^2 \\
&= (\det[(\sigma_i(\alpha_j))(c_{jk})])^2,
\end{aligned}$$

from which it follows that

$$\Delta[\beta_1, \dots, \beta_n] = \Delta[\alpha_1, \dots, \alpha_n] (\det(c_{jk}))^2. \quad (2.1)$$

A determinant of the form $D = \det(t_i^j)_{1 \leq i, j \leq n}$ is called a *Vandermonde* determinant, and has value:

$$D = (-1)^{\frac{n(n-1)}{2}} t_1 t_2 \cdots t_n \delta(t_1, \dots, t_n) = t_1 \cdots t_n \prod_{1 \leq j < i \leq n} (t_i - t_j), \quad (2.2)$$

where $\delta(t_1, \dots, t_n) = \prod_{1 \leq i < j \leq n} (t_i - t_j)$.

To see this, think of everything as lying inside $Q[t_1, \dots, t_n]$. Then for $t_i = t_j$ the determinant has two equal rows, so equals zero. Hence D is divisible by each $(t_i - t_j)$. To avoid repeating such a factor twice, we take $j < i$. Also, it is clear that D is divisible by each t_i . Then comparison of degrees easily shows that D has no other nonconstant factors: both degrees equal $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Comparing coefficients of $t_1 t_2^2 \cdots t_n^n$ gives the desired result.

From the above it follows easily that if

$$A = \begin{pmatrix} 1 & t_1 & t_1^2 & \cdots & t_1^{n-1} \\ 1 & t_2 & t_2^2 & \cdots & t_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & t_n & t_n^2 & \cdots & t_n^{n-1} \end{pmatrix},$$

then

$$\det(A) = \prod_{1 \leq j < i \leq n} (t_i - t_j). \quad (2.3)$$

Theorem 2.1.3. *The discriminant of any basis for $K = Q(\theta)$ is rational and non-zero. If all K -conjugates of θ are real, then the discriminant of any basis is positive.*

Proof. First we pick a basis with which we can compute: the obvious one is $\{1, \theta, \dots, \theta^{n-1}\}$. If the conjugates of θ are $\theta_1, \dots, \theta_n$, then

$$\Delta = \Delta[1, \theta, \dots, \theta^{n-1}] = \left[\prod_{1 \leq j < i \leq n} (\theta_i - \theta_j) \right]^2 = [\delta(\theta_1, \dots, \theta_n)]^2.$$

Clearly Δ is symmetric in the θ_i so that $\Delta \in Q$. Using Eq. 2.1 with $c_{jk} \in Q$ it is clear that the discriminant of any basis will be rational and non-zero. Moreover, if all the conjugates of θ are real, then the discriminant is the square of a real number and hence positive. \square

As usual, let $K = Q(\theta)$ be a number field of degree n and let $\sigma_1, \dots, \sigma_n$ be the monomorphisms $K \rightarrow C$. For any $\alpha \in K$ we define the *norm*

$$N_K(\alpha) = N(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

Since the σ_i are monomorphisms it is clear that

$$N(\alpha\beta) = N(\alpha)N(\beta), \quad (2.4)$$

and if $\alpha \neq 0$, then $N(\alpha) \neq 0$.

Similarly, the *trace* of α is defined by

$$Tr_K(\alpha) = Tr(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

It is clear that Tr is linear over Q , i.e.,

$$Tr(a\alpha + \beta) = aTr(\alpha) + Tr(\beta), \text{ for all } a \in Q, \alpha, \beta \in K. \quad (2.5)$$

Since both $N(\alpha)$ and $Tr(\alpha)$ are fixed by all monomorphisms of K into \mathcal{C} , clearly both $N(\alpha) \in Q$ and $Tr(\alpha) \in Q$.

From the proof of Theorem 2.1.3 we can derive another useful formula for the discriminant of the basis used in that theorem.

Theorem 2.1.4. *Let $K = Q(\theta)$ be a number field where θ has minimum polynomial p of degree n . The Q -basis $\{1, \theta, \dots, \theta^{n-1}\}$ has discriminant*

$$\Delta[1, \dots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)),$$

where p' is the formal derivative of p .

Proof. Since $p(x) = \prod_{i=1}^n (x - \theta_i)$, its derivative satisfies

$$p'(x) = \sum_{j=1}^n \prod_{\substack{i=1 \\ i \neq j}}^n (x - \theta_i),$$

from which it follows that

$$p'(\theta_j) = \prod_{\substack{i=1 \\ i \neq j}}^n (\theta_j - \theta_i).$$

Multiplying all these equations for $j = 1, \dots, n$ we obtain

$$\prod_{j=1}^n p'(\theta_j) = \prod_{\substack{i,j=1 \\ i \neq j}}^n (\theta_i - \theta_j).$$

The left-hand side is $N(p'(\theta))$. On the right, each factor $(\theta_i - \theta_j)$ for $i < j$ appears twice, once as $(\theta_i - \theta_j)$ and once as $(\theta_j - \theta_i)$. The product of these two factors is $-(\theta_i - \theta_j)^2$. On multiplying we obtain Δ multiplied by $(-1)^s$ where s is the number of pairs (i, j) with $1 \leq i < j \leq n$, which means $s = n(n-1)/2$, completing the proof. \square

2.2 Algebraic Integers

An *algebraic number* is a complex number α that is a root of a polynomial $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$, where $a_0, \dots, a_n \in Q$. Multiplying by the least common multiple of the denominators of the a_i 's leads to a polynomial in

$\mathcal{Z}[x]$ having α as a root. An *algebraic integer* w is a complex number that is the root of a *monic* polynomial (i.e., $a_n = 1$) with integer coefficients. Let Ω represent the set of all algebraic integers in \mathcal{C} .

The following result has simple proof.

Lemma 2.2.1. *A rational number $r \in Q$ is an algebraic integer if and only if $r \in \mathcal{Z}$.*

Definition: A nonempty subset V of the complex numbers is called a Q -*module* if the following three properties hold:

- (a) $\gamma_1, \gamma_2 \in V$ implies that $\gamma_1 \pm \gamma_2 \in V$.
- (b) $\gamma \in V$ and $r \in Q$ implies that $r\gamma \in V$.
- (c) There exist elements $\gamma_1, \dots, \gamma_l \in V$ such that every $\gamma \in V$ has the form $\sum_{i=1}^l r_i \gamma_i$ with $r_i \in Q$.

Briefly, we say that $V \subset \mathcal{C}$ is a Q -module provided it is a finite dimensional vector space over Q . If $\gamma_1, \gamma_2, \dots, \gamma_l \in \mathcal{C}$, the set of all expressions $\sum_{i=1}^l r_i \gamma_i$, $r_i \in Q$ is easily seen to be a Q -module. We denote this Q -module by $[\gamma_1, \dots, \gamma_l]$.

Theorem 2.2.2. *Let $V = [\gamma_1, \dots, \gamma_l]$, and suppose that $\alpha \in \mathcal{C}$ has the property that $\alpha\gamma \in V$ for all $\gamma \in V$. Then α is an algebraic number.*

Proof. $\alpha\gamma_i \in V$ for $i = 1, 2, \dots, l$. Thus $\alpha\gamma_i = \sum_{j=1}^l a_{ij}\gamma_j$, where $a_{ij} \in Q$. It follows that $0 = \sum_{j=1}^l (a_{ij} - \delta_{ij}\alpha)\gamma_j$, where $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j$. Hence $\det(a_{ij} - \delta_{ij}\alpha) = 0$. Writing out the determinant we see that α satisfies a polynomial of degree l with rational coefficients. Thus α is an algebraic number. \square

Theorem 2.2.3. *The set of algebraic numbers forms a field.*

Proof. If α_1 and α_2 are algebraic numbers we show that $\alpha_1\alpha_2$ and $\alpha_1 + \alpha_2$ are algebraic numbers. Suppose that $\alpha_1^n + r_1\alpha_1^{n-1} + \dots + r_n = 0$ and that $\alpha_2^m + s_2\alpha_2^{m-1} + \dots + s_m = 0$, where $r_i, s_j \in Q$. Let V be the Q -module obtained by forming all Q -linear combinations of the elements $\alpha_1^i\alpha_2^j$, where $0 \leq i < n$ and $0 \leq j < m$. For $\gamma \in V$ we have $\alpha_1\gamma \in V$ and $\alpha_2\gamma \in V$. For example, if $i < n - 1$, then $\alpha_1\alpha_1^i\alpha_2^j = \alpha_1^{i+1}\alpha_2^j \in V$. And if $i = n - 1$, so $i + 1 = n$, $\alpha_1\alpha_1^{n-1}\alpha_2^j = -r_1\alpha_1^{n-1}\alpha_2^j + \dots + -r_n\alpha_2^j \in V$. Thus we also have $(\alpha_1 + \alpha_2)\gamma \in V$ and $(\alpha_1\alpha_2)\gamma \in V$. By Theorem 2.2.2 it follows that both $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$ are algebraic numbers. Finally, if α is an algebraic number, not zero, we must show that α^{-1} is an algebraic number. Suppose

that $a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$, where the $a_i \in Q$ are not all zero. Then $a_n\alpha^{-n} + a_{n-1}\alpha^{-(n-1)} + \cdots + a_0 = 0$. The result follows. \square

To prove that the set of algebraic integers forms a ring it is necessary only to alter the above proofs slightly.

Definition: A subset $W \subseteq \mathcal{C}$ is called a \mathcal{Z} -module provided

(a) $\gamma_1, \gamma_2 \in W$ implies that $\gamma_1 \pm \gamma_2 \in W$.

(b) There exist elements $\gamma_1, \gamma_2, \dots, \gamma_l \in W$ such that every $\gamma \in W$ is of the form $\sum_{i=1}^l b_i \gamma_i$ with $b_i \in \mathcal{Z}$.

Theorem 2.2.4. *Let W be a \mathcal{Z} -module and suppose that $w \in \mathcal{C}$ is such that $w\gamma \in W$ for all $\gamma \in W$. Then w is an algebraic integer.*

Proof. The proof proceeds exactly as in the proof of Theorem 2.2.2, except that now $a_{ij} \in \mathcal{Z}$. The equation $\det(a_{ij} - \delta_{ij}w) = 0$, when written out, shows that w satisfies a monic equation of degree l with integer coefficients. Thus w is an algebraic integer. \square

Theorem 2.2.5. *The set of algebraic integers forms a ring Ω .*

Proof. The proof follows from Theorem 2.2.4 in exactly the same way in which the proof of Theorem 2.2.3 follows from Theorem 2.2.2. \square

Definition: A subfield K of the complex numbers is called an *algebraic number field* provided $[K : Q]$ is finite. If K is such a field, the subset of K consisting of algebraic integers forms a ring D called the ring of algebraic integers in K . Theorem 2.2.2 shows that an algebraic number field consists of algebraic numbers (just take $V = K$ and choose $\gamma_1, \dots, \gamma_n$ to be a basis for K over Q).

Theorem 2.2.6. *Suppose $\beta \in K$. There is an integer $b \in \mathcal{Z}$, $b \neq 0$, such that $b\beta \in D$.*

Proof. We know that β satisfies an equation $a_n\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_0 = 0$ with $a_i \in \mathcal{Z}$. Multiplying by a_n^{n-1} we get $(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + \cdots + a_0a_n^{n-1}(a_n\beta)^0 = 0$. Therefore $a_n\beta \in D$ since $a_i a_n^{i-1} \in \mathcal{Z}$. \square

Theorem 2.2.7. *Every (nonzero) ideal A of D contains a basis for K over Q .*

Proof. Let $\alpha_1, \dots, \alpha_n$ be a basis for K over Q . Then by Theorem 2.2.6 there exist some $a_i \in \mathcal{Z}$ such that $a_i \alpha_i \in D$, $a_i \neq 0$, $1 \leq i \leq n$. Let $a = \text{lcm}[a_1, a_2, \dots, a_n]$. Then $a\alpha_1, a\alpha_2, \dots, a\alpha_n \in D$. Pick $\beta \in A$, $\beta \neq 0$. We claim that $a\alpha_1\beta, a\alpha_2\beta, \dots, a\alpha_n\beta$ is a basis for K over Q (clearly contained in A). Suppose not. Then for $1 \leq i \leq n$ there exists $c_i \in Q$, not all $c_i = 0$, such that $\sum_{i=1}^n c_i a\alpha_i\beta = 0$, which implies that $a\beta \sum_{i=1}^n c_i \alpha_i = 0$, which is a contradiction that proves the theorem. \square

Theorem 2.2.8. *Let A be an ideal in D and suppose $\alpha_1, \dots, \alpha_n \in A$ is a basis for K over Q with $|\Delta[\alpha_1, \dots, \alpha_n]|$ minimal. Then $A = \mathcal{Z}\alpha_1 + \mathcal{Z}\alpha_2 + \dots + \mathcal{Z}\alpha_n$.*

Proof. By Theorem 2.1.3 $\Delta[\alpha_1, \dots, \alpha_n] \in Q \cap D = \mathcal{Z}$, so we may choose a basis with minimal discriminant as described in the theorem. Suppose $\alpha \in A$. Then $\alpha = \sum_{i=1}^n \gamma_i \alpha_i$, $\gamma_i \in Q$. We need to show that $\gamma_i \in \mathcal{Z}$. Suppose not. Then there exists i such that $\gamma_i \notin \mathcal{Z}$. Without loss of generality let this be γ_1 . Then we can write $\gamma_1 = m + \theta$, $m \in \mathcal{Z}$, $0 < \theta < 1$. Set $\beta_1 = \alpha - m\alpha_1 = \theta\alpha_1 + \sum_{i=2}^n \gamma_i \alpha_i \in A$, $\beta_i = \alpha_i$ for $2 \leq i \leq n$. We claim that $\beta_1, \beta_2, \dots, \beta_n$ is a basis for K over Q . Suppose not. Then there exist $c_1, \dots, c_n \in Q$ such that $\sum_{i=1}^n c_i \beta_i = 0$ which implies $c_1(\alpha - m\alpha_1) + \sum_{i=2}^n c_i \beta_i = 0$. Hence $c_1 \sum_{i=1}^n \gamma_i \alpha_i - c_1 m \alpha_1 + \sum_{i=2}^n c_i \beta_i = 0$, implying $(c_1 \gamma_1 - c_1 m) \alpha_1 + \sum_{i=2}^n (c_1 \gamma_i + c_i) \alpha_i = 0$. This implies that all the coefficients on the α_i must be zero. In particular, $c_1(\gamma_1 - m) = c_1 \theta = 0$, implying $c_1 = 0$, from which we see $\sum_{i=2}^n c_i \alpha_i = 0$, implying all the c_i are zero. Therefore β_1, \dots, β_n are linearly independent and hence form a basis for K over Q consisting of elements of A .

Since $\beta_1 = \alpha - m\alpha_1 = \sum_{i=1}^n \gamma_i \alpha_i - m\alpha_1 = \theta\alpha_1 + \gamma_2\alpha_2 + \dots + \gamma_n\alpha_n$. This gives the transition matrix M where

$$M^T = \begin{pmatrix} \theta & \gamma_2 & \gamma_3 & \cdots & \gamma_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & \vdots \\ \vdots & \vdots & & & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

By Eq. 2.1 $\Delta[\beta_1, \dots, \beta_n] = (\det M)^2 \Delta[\alpha_1, \dots, \alpha_n]$, yielding

$$\Delta[\beta_1, \dots, \beta_n] = \theta^2 \Delta[\alpha_1, \dots, \alpha_n],$$

and hence

$$|\Delta[\beta_1, \dots, \beta_n]| < |\Delta[\alpha_1, \dots, \alpha_n]|,$$

contradicting the original choice of basis. Thus $\gamma_i \in \mathcal{Z}$ for all i . Hence $A = \mathcal{Z}\alpha_1 + \cdots + \mathcal{Z}\alpha_n$. \square

Definition: If $\alpha_1, \dots, \alpha_n \in A$ is a basis for K over Q and $A = \mathcal{Z}\alpha_1 + \cdots + \mathcal{Z}\alpha_n$, then $\alpha_1, \dots, \alpha_n$ is called an *integral basis* for A . It follows from Theorem 2.2.8 that the discriminants of any two integral bases for A are equal. (To see this, suppose $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_n\}$ are two integral bases for A . If

$$\{\beta_1, \dots, \beta_n\} = \{\alpha_1, \dots, \alpha_n\}M, \quad \text{so } \{\alpha_1, \dots, \alpha_n\} = \{\beta_1, \dots, \beta_n\}M^{-1},$$

then both M and M^{-1} have entries from \mathcal{Z} . Then $\det(M)$ and $\det(M^{-1})$ must both be integers and inverses of each other. Hence the two determinants are both 1 or both -1. From this it follows that the bases have the same discriminant.) This common value is called the *discriminant of A* , written $\Delta(A)$. The discriminant of D is particularly important, and $\delta_K = \Delta(D)$ is called the discriminant of K/Q .

Lemma 2.2.9. *If $A \subset D$ is a nonzero ideal, then $A \cap \mathcal{Z} \neq \{0\}$.*

Proof. Let $\alpha \in A$, $\alpha \neq 0$. Then there exists some polynomial such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, $a_i \in \mathcal{Z}$. We may assume $a_0 \neq 0$, since otherwise we could simply factor out the appropriate power of α (so just use the minimal polynomial of α). Since $\alpha^n, a_i\alpha^i \in A$ we have $a_0 \in A$. Therefore $A \cap \mathcal{Z} \neq \{0\}$. \square

Theorem 2.2.10. *For any nonzero ideal A of D , D/A is finite. Moreover, if $A = (a)$ with $0 < a \in A$, and if n is the degree of the extension, then $|D/(a)| = a^n$.*

Proof. By Lemma 2.2.9 there exists an $a \in A \cap \mathcal{Z}$, $a \neq 0$. Let (a) be the principal ideal generated by a in D . Actually $(a) \subseteq A$, so there is an onto map from $D/(a)$ to D/A . Hence it suffices to show that $|D/(a)|$ is finite. In fact, we show that $|D/(a)| = a^n$. By Theorem 2.2.8 there is an integral basis w_1, \dots, w_n of D , so $D = \mathcal{Z}w_1 + \cdots + \mathcal{Z}w_n$.

Let

$$S = \left\{ \sum_{i=1}^n \gamma_i w_i : 0 \leq \gamma_i < a \right\}.$$

We claim that S is a complete set of coset representatives for $D/(a)$. Let $w = \sum_{i=1}^n m_i w_i$. Since $m_i \in \mathcal{Z}$, write $m_i = q_i a + \gamma_i$ with $0 \leq \gamma_i < a$. So

$w = \sum_{i=1}^n (q_i a + \gamma_i) w_i \equiv \sum_{i=1}^n \gamma_i w_i \pmod{(a)}$, so every coset of A contains an element of S .

Suppose $\sum_{i=1}^n \gamma_i w_i$ and $\sum_{i=1}^n \gamma'_i w_i$ are in the same coset modulo (a) . Then $\sum_{i=1}^n (\gamma_i - \gamma'_i) w_i \equiv 0 \pmod{(a)}$, which implies $\sum_{i=1}^n (\gamma_i - \gamma'_i) w_i = a\beta$ where $\beta \in D$. Using the fact that the w_i 's form an integral basis for D , we see that each $\gamma_i - \gamma'_i$ is divisible by a in \mathcal{Z} . Since $0 \leq \gamma_i, \gamma'_i < a$, it follows that $\gamma_i = \gamma'_i$. Thus S is a complete set of distinct coset representatives and $D/(a)$ has a^n elements as claimed. \square

We define a ring R to be a *Noetherian ring* if every ascending chain $A_1 \subset A_2 \subset \cdots$ of ideals terminates. In other words, there is an $N > 0$ such that $A_m = A_{m+1}$ for all $m \geq N$.

Corollary 2.2.11. *D is a Noetherian ring.*

Proof. Consider the chain of ideals $A_1 \subset A_2 \subset \cdots$ of D . If $A_i \subset A_{i+1}$ with $A_i \neq A_{i+1}$, then $|D/A_i| > |D/A_{i+1}|$. Since $|D/A_1|$ is finite, the chain of ideals containing A_1 must be finite. (Here we use the fact that if A and B are ideals in D with $A \subseteq B$ and $|D/A| = |D/B|$, then $A = B$. This follows from $(D/A)/(B/A) \cong D/B$.) \square

A proper ideal P of D is said to be a *prime ideal* of D if, for $a, b \in D$, whenever $ab \in P$ then $a \in P$ or $b \in P$. A proper ideal P of D is said to be a *maximal ideal* of D if, whenever A is an ideal of D with $P \subseteq A \subseteq D$, then $A = P$ or $A = D$.

Theorem 2.2.12. *An ideal $P \subset D$ is prime if and only if it is maximal.*

Proof. P is a prime ideal iff D/P is a finite integral domain iff D/P is a (finite) field iff P is a maximal ideal. \square

Lemma 2.2.13. *Let $A \subseteq D$ be an ideal. If $\beta \in K$ is such that $\beta A \subseteq A$, then $\beta \in D$.*

Proof. This is an immediate consequence of Theorems 2.2.4 and 2.2.8, since Theorem 2.2.8 says A is a \mathcal{Z} -module and Theorem 2.2.4 then says that $\beta \in D$. \square

Let A and B be ideals in D . Define the product of A and B to be

$$AB = \{a_1 b_1 + a_2 b_2 + \cdots + a_k b_k : a_i \in A; b_i \in B, k \in \mathcal{Z}^+\}$$

Lemma 2.2.14. *If A and B are ideals in D and $A = AB$, then $B = D$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be an integral basis for A . Since $A = AB$ we can find elements $b_{ij} \in B$ such that $\alpha_i = \sum_j b_{ij}\alpha_j$. In matrix form this says that $((b_{ij}) - I)[\alpha_1, \dots, \alpha_n]^T = [0, \dots, 0]^T$, implying $\det((b_{ij}) - I) = 0$. Writing out this determinant shows that $\pm 1 \in B$, i.e., $B = D$. \square

Theorem 2.2.15. *Let $A, B \subseteq D$ be ideals and suppose that $w \in D$ is such that $(w)A = BA$. Then $(w) = B$.*

Proof. If $\beta \in B$ then $(\beta)A \subseteq BA = (w)A$, so we see that $(\beta/w)A \subseteq A$. Hence by Lemma 2.2.13, $\beta/w \in D$. It follows that $B \subseteq (w)$, implying $w^{-1}B \subseteq D$ is an ideal. Since $A = w^{-1}BA$, Lemma 2.2.14 shows that $w^{-1}B = D$, so $B = (w)$ as required. \square

Recall that a *Galois* extension K of Q is a finite extension such that if G is the group of automorphisms of K , then Q is the fixed field of G . An equivalent property is that if an irreducible polynomial $f(x) \in Q[x]$ has one zero in K , then all of its zeros are in K . The group of automorphisms of K/Q is called the *Galois Group of K over Q* . By the fundamental theorem of Galois theory we have that $|G| = n = [K : Q]$.

The following definition plays a major role in algebraic number theory.

Definition: Two ideals $A, B \subseteq D$ are said to be equivalent, written $A \sim B$, provided there exist nonzero $\alpha, \beta \in D$ such that $(\alpha)A = (\beta)B$. This is an equivalence relation. The equivalence classes are called *ideal classes*. The number h_K of ideal classes is called the *class number* of K . Soon we will prove that the class number is finite. The reader should prove that \sim is an equivalence relation. It is also important to notice that $h_K = 1$ if and only if D is a principal ideal domain (PID). To see this, suppose that $h_K = 1$. Let A be an ideal in D . Since $A \sim D$ there are nonzero α and β in D such that $(\alpha)A = (\beta)D = (\beta)$. Thus $\frac{\beta}{\alpha} \in D$ and $(\frac{\beta}{\alpha}) = A$. Hence every ideal is principal. Conversely, it is obvious that if D is a PID then $h_K = 1$, since in general any principal ideal is equivalent to D .

Theorem 2.2.16. *There exists a positive integer M depending only on K with the following property. Given $\alpha, \beta \in D$, $\beta \neq 0$, there is an integer t , $1 \leq t \leq M$, and an element $w \in D$ such that $|N(t\alpha - w\beta)| < |N(\beta)|$.*

Proof. Let $\gamma = \frac{\alpha}{\beta} \in K$. Then $\beta^{-1}(t\alpha - w\beta) = t \cdot \frac{\alpha}{\beta} - w = t\gamma - w$, and $\beta^{-1}\beta = 1$, so it is sufficient to show that there exists a positive integer M such that for all $\gamma \in K$

$$|N(t\gamma - w)| < |N(1)| = 1$$

for some t , $1 \leq t \leq M$ and some $w \in D$. Let w_1, \dots, w_n be an integral basis for D . So we have that for all $\alpha \in D$, $\alpha = \sum_{i=1}^n \alpha_i w_i$, $\alpha_i \in \mathcal{Z}$ and for all $\gamma \in K$, $\gamma = \sum_{i=1}^n \gamma_i w_i$, $\gamma_i \in \mathcal{Q}$. Consider $\sigma_j(\gamma)$ where $\sigma_j \in G$. Since $\gamma_i \in \mathcal{Q}$,

$$\sigma_j(\gamma) = \sum_{i=1}^n \gamma_i \sigma_j(w_i).$$

So

$$\begin{aligned} |N(\gamma)| &= \left| \prod_{j=1}^n \sigma_j(\gamma) \right| = \prod_{j=1}^n \left| \sum_{i=1}^n \gamma_i \sigma_j(w_i) \right| \leq \\ &\prod_{j=1}^n \sum_{i=1}^n |\gamma_i \sigma_j(w_i)| \leq \prod_{j=1}^n \sum_{i=1}^n \max_i (|\gamma_i|) |\sigma_j(w_i)| = \\ &= (\max_i (|\gamma_i|))^n \prod_{j=1}^n \sum_{i=1}^n |\sigma_j(w_i)|. \end{aligned}$$

Let $C = \prod_{j=1}^n \sum_{i=1}^n |\sigma_j(w_i)|$, so that

$$|N(\gamma)| \leq C \cdot (\max_i (|\gamma_i|))^n.$$

Now choose $m \in \mathcal{Z}$ so that $M = m^n > C$. For $\gamma \in K$, $\gamma = \sum_{i=1}^n \gamma_i w_i$, let $\gamma_i = a_i + b_i$, $a_i \in \mathcal{Z}$, $0 \leq b_i < 1$. So $\gamma = \sum_{i=1}^n a_i w_i + \sum_{i=1}^n b_i w_i$. Let $[\gamma] = \sum_{i=1}^n a_i w_i$ and $\{\gamma\} = \sum_{i=1}^n b_i w_i$. Therefore $\gamma = [\gamma] + \{\gamma\}$ and $[\gamma] \in D$ since $a_i \in \mathcal{Z}$ and w_1, \dots, w_n is an integral basis for D . Let

$$\phi : K \rightarrow R^n : \sum_{i=1}^n \gamma_i w_i \mapsto (b_1, \dots, b_n).$$

Then for any γ , $\phi(\{\gamma\})$ lies in the unit cube since $0 \leq b_i < 1$. We will now partition the unit cube into m^n subcubes with sides of length $\frac{1}{m}$. Consider the points $\phi(\{k\gamma\})$ for $k = 1, \dots, m^n + 1$. Each $\phi(\{k\gamma\})$ will lie in one of the m^n subcubes, and because we are picking $m^n + 1$ points at least two of these points must lie in the same subcube. Call these $h\gamma$ and $l\gamma$ and write $h\gamma = [h\gamma] + \{h\gamma\}$ and $l\gamma = [l\gamma] + \{l\gamma\}$. Without loss of generality let $h > l$ and put $t = h - l$. Then $t\gamma = [h\gamma] - [l\gamma] + \{h\gamma\} - \{l\gamma\}$. Let $w = [h\gamma] - [l\gamma]$ and

$\delta = \{h\gamma\} - \{l\gamma\}$, so $t\gamma = w + \delta$. Note that $w = \sum_{i=1}^n ha_i w_i - \sum_{i=1}^n la_i w_i = (h-l)\sum_{i=1}^n a_i w_i \in D$. As far as δ is concerned, since $\{h\gamma\}$ and $\{l\gamma\}$ are in the same subcube the coordinates of δ must differ by less than $\frac{1}{m}$. So $|N(\delta)| \leq C(\max_i(|\delta_i|))^n \leq C(\frac{1}{m})^n < 1$ by choice of m . Hence

$$|N(\delta)| = |N(t\gamma - w)| < 1.$$

□

Theorem 2.2.17. *The class number of K is finite.*

Proof. Let A be an ideal in D . For all $\alpha \in A$, $\alpha \neq 0$, we have $|N(\alpha)| \in \mathcal{Z}^+$. Choose nonzero $\beta \in A$ so that $|N(\beta)|$ is minimal. Then by Theorem 2.2.16 for all $\alpha \in A$ there exists an integer t , $1 \leq t \leq M$ (for the M of the preceding theorem) such that $|N(t\alpha - w\beta)| < |N(\beta)|$ with $w \in D$ and $M \in \mathcal{Z}^+$. Since $t\alpha - w\beta \in A$ and $|N(\beta)|$ is minimal, then $t\alpha - w\beta = 0$, i.e., $t\alpha = w\beta$, which implies $t\alpha \in (\beta)$. Note that different elements in A may have different t values, $1 \leq t < M$. Since $M!$ is divisible by all of the possible t values, we have that for any $\alpha \in A$, $M!\alpha \in (\beta)$.

Let $B = \left(\frac{1}{\beta}\right)M!A \subseteq D$. Since B is a product of ideals it is also an ideal itself. Then $M!A = (\beta)\left(\frac{1}{\beta}\right)M!A = (\beta)B$ and hence $A \sim B$. Since $\beta \in A$ we have

$$M!\beta = \beta_1 b_1 + \cdots + \beta_k b_k, \quad \beta_i \in (\beta), \quad b_i \in B.$$

Hence we can write $\beta_i = \beta\beta'_i$ so we can divide both sides of the equation by β to get

$$M! = \beta'_1 b_1 + \cdots + \beta'_k b_k \in B.$$

But there can only be finitely many ideals containing $M!$, since $|D/(M!)|$ is finite and there is a bijection between the ideals of D containing $(M!)$ and the ideals of $D/(M!)$. Hence there are only finitely many choices for the ideal B containing $M!$ with $A \sim B$. In other words each ideal A is equivalent to one of the finitely many ideals containing $M!$, and the class number must be finite. □

Theorem 2.2.18. *For any ideal $A \subseteq D$ there is an integer k , $1 \leq k \leq h_K$, such that A^k is principal.*

Proof. Consider the set of ideals $\{A^i : 1 \leq i \leq h_K + 1\}$. Then there exist i, j , $i \neq j$ such that $A^i \sim A^j$. Without loss of generality let $i < j$. Then

there exist $\alpha, \beta \in D$, $\alpha, \beta \neq 0$ such that $(\alpha)A^i = (\beta)A^j$. Let $k = j - i$ and $B = A^k$. Then $(\alpha)A^i = (\beta)A^j = (\beta)A^k A^i = (\beta)BA^i$.

An arbitrary element in $(\alpha)A^i$ is of the form αa where $a \in A^i$. So $\alpha a = \beta \sum_j b_j a'_j$, $b_j \in B$, $a'_j \in A^i$, giving $\frac{\alpha}{\beta} a = \sum_j b_j a'_j$. Since $\frac{\alpha}{\beta} a$ is a general element of $\left(\frac{\alpha}{\beta}\right)A^i$, we have that $\left(\frac{\alpha}{\beta}\right)A^i \subseteq BA^i \subseteq A^i$. So by Lemma 2.2.13 $\frac{\alpha}{\beta} \in D$. Therefore by Theorem 2.2.15 $\left(\frac{\alpha}{\beta}\right) = B$, proving that B is principal. \square

Theorem 2.2.19. *If A , B and C are ideals, and $AB = AC$, then $B = C$.*

Proof. By Theorem 2.2.18 there exists some k such that $A^k = (\alpha)$. Then multiplying both sides of $AB = AC$ by A^{k-1} we get $(\alpha)B = (\alpha)C$. Pick $b \in B$. Then $\alpha b = \alpha c$ for some $c \in C$. Thus $b = c$ implies $B \subseteq C$. Similarly, $C \subseteq B$, and hence $B = C$. \square

Theorem 2.2.20. *If A and B are ideals such that $A \subseteq B$, then there is an ideal C such that $A = BC$.*

Proof. By Theorem 2.2.18 there exists some $k > 0$ such that $B^k = (\beta)$. Since $A \subseteq B$ we have $B^{k-1}A \subseteq B^k = (\beta)$. Put $C = \left(\frac{1}{\beta}\right)B^{k-1}A \subseteq D$. Then $BC = B\left(\frac{1}{\beta}\right)B^{k-1}A = \left(\frac{1}{\beta}\right)(\beta)A = A$. \square

This proposition is often stated as: “Containing is dividing.”

Theorem 2.2.21. *Every ideal in D can be written as a product of prime ideals.*

Proof. Let A be a proper ideal. Since D/A is finite, A is contained in a maximal ideal P_1 . (Using Zorn’s lemma one can show that in an arbitrary commutative ring with identity a proper ideal is contained in a maximal ideal.) By the preceding theorem $A = P_1 B_1$ for some ideal B_1 . If $B_1 \neq D$, then B_1 is contained in a maximal ideal P_2 , implying $A = P_1 P_2 B_2$. If $B_2 \neq D$, we can continue the process. Notice that $A \subset B_1 \subset B_2 \cdots$ is a proper ascending chain of ideals. Since D is Noetherian, we see that in finitely many steps $B_t = D$. Thus $A = P_1 P_2 \cdots P_t$. \square

Let P be a prime ideal. The descending chain $P \supseteq P^2 \supseteq \cdots$ is proper, since if $P^i = P^{i+1}$ for some i , then $PP^i = P^i$, forcing $P = D$ by Lemma 2.2.14. This allows us to give the following definition:

Definition: Let P be a prime ideal and A an ideal. Then $\text{ord}_P A$ is defined to be the unique nonnegative integer t such that $P^t \supseteq A$ and $P^{t+1} \not\supseteq A$.

Theorem 2.2.22. *Let P be a prime ideal and A and B ideals. Then*

- (i) $\text{ord}_P P = 1$;
- (ii) If $P' \neq P$ is prime, $\text{ord}_P P' = 0$;
- (iii) $\text{ord}_P AB = \text{ord}_P A + \text{ord}_P B$.

Proof. The first assertion is clear. For (ii), if $\text{ord}_P P' > 0$, then $P \supseteq P'$. Since prime ideals are maximal, $P = P'$, contradicting the hypothesis.

Let $t = \text{ord}_P A$ and $s = \text{ord}_P B$. By Theorem 2.2.20 we have $A = P^t A_1$ and $B = P^s B_1$. By the same proposition we have $P \not\supseteq A_1$ and $P \not\supseteq B_1$. Now, $AB = P^{s+t} A_1 B_1$. If $P^{s+t+1} \supseteq AB$ then $AB = P^{s+t+1} C$ and so by Theorem 2.2.19, $PC = A_1 B_1$. This implies $P \supseteq A_1 B_1$. Since P is prime, this means that $P \supseteq A_1$ or $P \supseteq B_1$, which is a contradiction. (To see this, suppose $B \not\subseteq P$ and let $b \in B \setminus P$. Then $AB \subseteq P$ implies that $ab \in P$ for all $a \in A$. This forces $a \in P$ for all $a \in A$, i.e., $A \subseteq P$, a contradiction.)

Hence $\text{ord}_P AB = t + s = \text{ord}_P A + \text{ord}_P B$. □

Theorem 2.2.23. *Let $A \subseteq D$ be an ideal. Then $A = \prod P^{a(P)}$, where the product is over all distinct prime ideals of D , and the $a(P)$ are nonnegative integers, all but finitely many of which are zero. Finally, the integers $a(P)$ are uniquely determined by $a(P) = \text{ord}_P A$.*

Proof. The product representation follows from Theorem 2.2.21.

Let P_0 be a prime ideal and apply ord_{P_0} to both sides of the product given in the theorem. Using Theorem 2.2.22 we see

$$\text{ord}_{P_0} A = \sum_P a(P) \text{ord}_{P_0}(P) = a(P_0).$$

□

2.3 Ramification and Degree

Let P be a prime ideal of D . By Lemma 2.2.9 $P \cap \mathcal{Z}$ is not zero. Since it is clearly a prime ideal of \mathcal{Z} we must have

$$P \cap \mathcal{Z} = (p) \quad \text{where } p \text{ is a prime number.}$$

Definition: The number $e = \text{ord}_P(p)$ is called the *ramification index* of P . D/P is a finite field containing $\mathcal{Z}/p\mathcal{Z}$. (To see this, consider the map $D \rightarrow D/P : d \mapsto d + P$ restricted to $Z : n \mapsto n + P$ which is the identity if and only if $n \in P \cap \mathcal{Z} = p\mathcal{Z}$, so that $Z/pZ \subseteq D/P$. Thus the number of elements in D/P is of the form p^f for some $f \geq 1$. The number f is called the *degree* of P .

Let $p \in \mathcal{Z}$ be a prime number and let P_1, P_2, \dots, P_g be the primes in D containing (p) . Let e_i and f_i be the ramification index and degree of P_i , respectively. By Theorem 2.2.23, $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$.

Theorem 2.3.1. (*Chinese Remainder Theorem*) *Let R be a commutative ring with identity. Suppose A_1, A_2, \dots, A_g are ideals such that $A_i + A_j = R$ for $i \neq j$. Let $A = A_1 A_2 \cdots A_g$. Then*

$$R/A \cong R/A_1 \oplus R/A_2 \oplus \cdots \oplus R/A_g.$$

Proof. Let ψ_i be the natural map from R to R/A_i and define $\psi : R \rightarrow R/A_1 \oplus \cdots \oplus R/A_g$ by $\psi(\gamma) = (\psi_1(\gamma), \psi_2(\gamma), \dots, \psi_g(\gamma))$. We will show that ψ is onto and its kernel is A . It is easy to see that ψ is a homomorphism. To show that ψ is onto it is sufficient to show that for any $\gamma_1, \dots, \gamma_g \in R$, the set of simultaneous congruences $x \equiv \gamma_i \pmod{A_i}$, $i = 1, \dots, g$, is solvable.

Expanding the product $(A_1 + A_2)(A_1 + A_3) \cdots (A_1 + A_g) = R$ we see that all the summands except the last are in A_1 . Thus $A_1 + A_2 \cdots A_g = R$. There exist elements $v_1 \in A_1$ and $u_1 \in A_2 \cdots A_g$ such that $u_1 + v_1 = 1$. Then $u_1 \equiv 1 \pmod{A_1}$ and $u_1 \equiv 0 \pmod{A_i}$ for $i \neq 1$. Similarly, for each j there is a u_j such that $u_j \equiv 1 \pmod{A_j}$ and $u_j \equiv 0 \pmod{A_i}$ for $i \neq j$. Then it is clear that $x = \sum_{i=1}^g \gamma_i u_i$ is a solution to our system of congruences. Hence ψ is onto.

Clearly, $\ker(\psi) = A_1 \cap A_2 \cap \cdots \cap A_g$. We must show that under the present hypotheses the intersection is equal to the product. This can be done by induction on g . Suppose $g = 2$. Then, since $A_1 + A_2 = R$, there exist $a_1 \in A_1$ and $a_2 \in A_2$ such that $a_1 + a_2 = 1$. If $a \in A_1 \cap A_2$ then $a = aa_1 + aa_2 \in A_1 A_2$. This shows that $A_1 \cap A_2 \subseteq A_1 A_2$. The reverse inclusion is obvious, so the result follows for $g = 2$. Now suppose $g > 2$ and we know the result for $g - 1$. Then $A_1 \cap A_2 \cap \cdots \cap A_g = A_1 \cap A_2 \cdots A_g$. However, $A_1 + A_2 A_3 \cdots A_g = R$ by the first part of the proof. Hence $A_1 \cap A_2 A_3 \cdots A_g = A_1 A_2 \cdots A_g$ and the proof is complete. \square

Theorem 2.3.2. *Let $P \subseteq D$ be a prime ideal and let p^f be the number of elements in D/P . The number of elements in D/P^e is p^{ef} .*

Proof. The assertion is clearly true for $e = 1$. If $e > 1$, then D/P^e has P^{e-1}/P^e as a subgroup and the quotient group is isomorphic to D/P^{e-1} (second law of isomorphisms). If we can show P^{e-1}/P^e has p^f elements, then the result will follow by induction.

Since $P^e \subset P^{e-1}$ (proper containment) we can find an $\alpha \in P^{e-1} \setminus P^e$. We claim $(\alpha) + P^e = P^{e-1}$. Since $P^e \subseteq \alpha + P^e$, the latter ideal must be a power of P . Since $(\alpha) + P^e \subseteq P^{e-1}$, we must have $(\alpha) + P^e = P^{e-1}$.

Map $D \rightarrow P^{e-1}/P^e$ by $\gamma \mapsto \gamma\alpha + P^e$. This is easily seen to be a homomorphism onto. For suppose $\beta \in P^{e-1} \setminus P^e$. Then $\beta \in (\beta) + P^e = (\alpha) + P^e$, so $\beta = \gamma\alpha + w$, $w \in P^e$. Hence $\beta + P^e = \gamma\alpha + P^e$.

An element γ is in the kernel if and only if $\gamma\alpha \in P^e$, i.e., iff $\text{ord}_P(\gamma\alpha) \geq e$. Now, $\text{ord}_P(\gamma\alpha) = \text{ord}_P(\gamma) + \text{ord}_P(\alpha) = \text{ord}_P(\gamma) + e - 1$. Thus γ is in the kernel iff $\text{ord}_P(\gamma) \geq 1$, which is equivalent to saying $\gamma \in P$. Thus $D/P \cong P^{e-1}/P^e$, implying that the latter group has p^f elements. \square

Lemma 2.3.3. *If P_i and P_j are distinct prime ideals in D and a and b are positive integers, then $P_i^a + P_j^b = D$.*

Proof. Suppose there is a prime ideal P' such that $P_i^a \subseteq P'$ and $P_j^b \subseteq P'$. Without loss of generality consider $P_i^a \subseteq P'$. (Recall that if $AB \subseteq P'$, then $A \subseteq P'$ or $B \subseteq P'$. Hence if $P_i^a \subseteq P'$, a finite induction shows that $P_i \subseteq P'$, i.e., $P_i = P'$. A similar argument shows that $P_j = P'$, which is a contradiction. \square

Theorem 2.3.4. *Recall that $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Then $\sum_{i=1}^g e_i f_i = n$.*

Proof. By the preceding lemma we see that $P_i^{e_i} + P_j^{e_j} = D$ for $i \neq j$. By Theorem 2.3.1

$$D/(p) \cong D/P_1^{e_1} \oplus \cdots \oplus D/P_g^{e_g}.$$

The proof of Theorem 2.2.10 shows that $|D/(p)| = p^n$. On the other hand Theorem 2.3.2 shows that $|D/P_i^{e_i}| = p^{e_i f_i}$. Thus

$$p^n = p^{e_1 f_1} p^{e_2 f_2} \cdots p^{e_g f_g},$$

so that $n = e_1 f_1 + e_2 f_2 + \cdots + e_g f_g$ as asserted. \square

Theorem 2.3.5. *Let p be a rational prime. Suppose that P_i and P_j are prime ideals of D containing p . Then there is a $\sigma \in G$ such that $\sigma(P_i) = P_j$.*

Proof. Suppose there is a prime ideal P_0 containing p and not in the set $\{\sigma(P_i) : \sigma \in G\}$. We saw in the proof of the Chinese Remainder Theorem that there exists $\alpha \in D$ such that $\alpha \equiv 0 \pmod{P_0}$ and $\alpha \equiv 1 \pmod{\sigma(P_i)}$ for all $\sigma \in G$. Then $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. The identity mapping gives us a term in P_0 . Since $N(\alpha) \in \mathcal{Z}$ we have $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \in P_0 \cap \mathcal{Z}$. However, since $p \in P_0$ we have that $N(\alpha) \in p\mathcal{Z}$, and since $p \in P_i$ we have $N(\alpha) \in P_i$. The fact that P_i is prime implies that for some $\sigma \in G$, $\sigma(\alpha) \in P_i$. However this implies $\alpha \in \sigma^{-1}(P_i)$, implying $\alpha \equiv 0 \pmod{\sigma^{-1}(P_i)}$, which is a contradiction. \square

Theorem 2.3.6. *Suppose K/Q is a Galois extension. Let p be a rational prime with*

$$(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}. \quad (2.6)$$

Then $e_1 = e_2 = \cdots = e_g$ and $f_1 = f_2 = \cdots = f_g$. If e and f denote these common values, then $efg = n$.

Proof. By the previous theorem we have that there is a $\sigma \in G$ such that $\sigma(P_1) = P_i$. Also, it is easy to check that for $\sigma \in G$, $\hat{\sigma} : D/P_1 \rightarrow D/P_i : \alpha + P_1 \mapsto \sigma(\alpha) + P_i$ is an isomorphism. Hence $p^{f_1} = |D/P_1| = |D/P_i| = p^{f_i}$, implying $f_1 = f_2 = \cdots = f_g$. Let f denote the common value.

To show that $e_1 = e_2 = \cdots = e_g$ apply σ to both sides of Eq. 2.6. Since $p \in \mathcal{Z}$ we get

$$(p) = \sigma(p) = \sigma(P_1^{e_1} \cdots P_g^{e_g}) = (\sigma(P_1))^{e_1} \cdots (\sigma(P_g))^{e_g}.$$

In this product we have e_1 as the exponent on $P_i = \sigma(P_1)$. Since prime factorization is unique we must have $e_1 = e_i$. It follows that all the e_i are the same, with common value e . It then follows that $n = \sum e_i f_i = efg$. \square

Recapitulation: Let K/Q be an algebraic number field with $[K : Q] = n$ and let D be the ring of algebraic integers in K . Given a rational prime p ,

$$(p) = (P_1 P_2 \cdots P_g)^e \quad \text{with } |D/P_i| = p^f \text{ and } efg = n.$$

We say that P is *ramified* if $e > 1$.

Chapter 3

Cyclotomic Fields

3.1 Roots of Unity

Let m be a positive integer and put $\zeta_m = e^{2\pi i/m}$. The number ζ_m generates the cyclic multiplicative group of complex m th roots of 1, i.e., the group of roots of $x^m - 1 = 0$. Hence

$$x^m - 1 = (x - 1)(x - \zeta_m) \cdots (x - \zeta_m^{m-1}).$$

It follows that the field $K = Q(\zeta_m)$ is the splitting field of the polynomial $x^m - 1$. Thus K/Q is a Galois extension.

We call $K = Q(\zeta_m)$ the *cyclotomic field of m th roots of unity*.

Theorem 3.1.1. *Let G be the Galois group of K/Q . There is a monomorphism $\theta : G \rightarrow U(\mathcal{Z}/m\mathcal{Z})$ such that for $\sigma \in G$*

$$\sigma(\zeta_m) = \zeta_m^{\theta(\sigma)}.$$

Proof. Since $\zeta_m^m = 1$ we have $(\sigma(\zeta_m))^m = 1$. Thus $\sigma(\zeta_m) = \zeta_m^{\theta(\sigma)}$ where $\theta(\sigma)$ is an integer modulo m . If $\tau = \sigma^{-1}$ then $\zeta_m = \tau\sigma\zeta_m = \tau(\zeta_m^{\theta(\sigma)}) = \zeta_m^{\theta(\tau)\theta(\sigma)}$. Thus $\theta(\tau)\theta(\sigma) = \bar{1}$ (where $\bar{1}$ is the coset of 1 in $\mathcal{Z}/m\mathcal{Z}$). Thus $\theta : G \rightarrow U(\mathcal{Z}/m\mathcal{Z})$. It is easily checked that θ is a homomorphism. For let $\sigma, \tau \in G$, so $\sigma \cdot \tau \in G$ and $(\sigma \cdot \tau)\zeta_m = \zeta_m^{\theta(\sigma \cdot \tau)}$. But we also have $(\tau \cdot \sigma)\zeta_m = \tau(\zeta_m^{\theta(\sigma)}) = \zeta_m^{\theta(\sigma)\theta(\tau)}$. Hence $\zeta_m^{\theta(\sigma \cdot \tau)} = \zeta_m^{\theta(\sigma)\theta(\tau)}$, which implies $\theta(\sigma \cdot \tau) \equiv \theta(\sigma)\theta(\tau) \pmod{m}$. Finally, if $\theta(\sigma) = \bar{1}$, then $\sigma(\zeta_m) = \zeta_m$, implying that σ is the identity of G since ζ_m generates K over Q . \square

Corollary 3.1.2. $[Q(\zeta_m) : Q]$ divides $\phi(m)$.

Proof. The order of G divides the order of $U(\mathcal{Z}/m\mathcal{Z})$ which equals $\phi(m)$. \square

Definition: Let $\Phi_m(x) = \prod_{(n,m)=1} (x - \zeta_m^n)$.

Note that the roots of the m th cyclotomic polynomial are exactly the primitive m th roots of unity. We define D_m to be the ring of algebraic integers in $Q(\zeta_m)/Q$.

Theorem 3.1.3. $X^m - 1 = \prod_{d|m} \Phi_d(x)$. If $m = p^r$ with p a prime, then $x^m - 1 = \prod_{i=0}^{r-1} \Phi_{p^i} = (x^{m/p} - 1)\Phi_m$.

Proof.

$$x^m - 1 = \prod_{d|m} \prod_{(i,m)=d} (x - \zeta_m^i).$$

We claim $\prod_{(i,m)=d} (x - \zeta_m^i) = \Phi_{m/d}(x)$. The Theorem will follow from this.

If $(i, m) = d$, let $i = dj$. Then $\zeta_m^i = \zeta_m^{dj} = \zeta_{m/d}^j$. Moreover, $(j, m/d) = 1$. Thus $\prod_{(i,m)=d} (x - \zeta_m^i) = \prod_{(j,m/d)=1} (x - \zeta_{m/d}^j) = \Phi_{m/d}(x)$. \square

Corollary 3.1.4. $\Phi_m(x) \in \mathcal{Z}[x]$.

Proof. Proceed by induction on m . $\phi_1(x) = x - 1$, which shows that the corollary is true for $m = 1$. Now suppose the corollary has been established for integers less than m . By the theorem, $\Phi_m(x) = (x^m - 1)/f(x)$, where $f(x)$ is a monic polynomial which by the induction hypothesis is in $\mathcal{Z}[x]$. It follows by “long division” that $\Phi_m(x) \in \mathcal{Z}[x]$. \square

From now on we let $p \in \mathcal{Z}$ be a prime such that p does not divide m and $P \subset D_m$ be a prime ideal of D_m containing p . We will also let F be a finite field of order p^f that is isomorphic to D_m/P .

Theorem 3.1.5. The cosets containing $1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}$ in D_m/P are all distinct and are the m distinct m th roots of 1 in D_m/P . If f denotes the degree of P , then $p^f \equiv 1 \pmod{(m)}$.

Proof. For $w \in D_m$ let \bar{w} denote its coset in D/P .

Divide both sides of $x^m - 1 = \prod (x - \zeta_m^i)$ by $x - 1$. We find

$$1 + x + \dots + x^{m-1} = \prod_{i=1}^{m-1} (x - \zeta_m^i).$$

Let $x = 1$ in this identity to obtain $m = \prod(1 - \zeta_m^i)$, where $1 \leq i \leq m - 1$. Therefore $\bar{m} = \prod(1 - \bar{\zeta}_m^i)$. Since $\bar{m} \neq \bar{0}$ it follows that $\bar{\zeta}_m^i \neq \bar{1}$ for $1 \leq i \leq m - 1$, so that $\bar{\zeta}_m^i \neq \bar{\zeta}_m^j$ for $0 \leq i, j \leq m - 1$. The elements $\{\bar{\zeta}_m^i : 0 \leq i \leq m - 1\}$ form a subgroup of order m in the multiplicative group of D_m/P . The latter group has order $p^f - 1$. Therefore $p^f \equiv 1 \pmod{(m)}$. \square

Theorem 3.1.6. *The m th cyclotomic polynomial $\Phi_m(x)$ is irreducible in $\mathcal{Z}[x]$.*

Proof. See p. 195 of Ireland and Rosen. \square

Corollary 3.1.7. $[Q(\zeta_m) : Q] = \phi(m)$.

Corollary 3.1.8. *The map θ of Theorem 3.1.1 is an isomorphism of G onto $U(\mathcal{Z}/m\mathcal{Z})$.*

Proof. Both G and $U(\mathcal{Z}/m\mathcal{Z})$ have $\phi(m)$ elements. Since θ is one-to-one it must be onto. \square

By the preceding Corollary we see that for every $a \in \mathcal{Z}$ with $(a, m) = 1$ there is a $\sigma_a \in G$ such that $\sigma_a(\zeta_m) = \zeta_m^a$. The map $a \mapsto \sigma_a$ gives rise to a homomorphism from $U(\mathcal{Z}/m\mathcal{Z})$ to G which is inverse to θ . If p is a prime not dividing m , we wish to study more closely the automorphism σ_p after some preliminary work.

3.2 Algebra in D_m

We start with a more general lemma.

Lemma 3.2.1. *Let K/Q be an algebraic number field of degree n . Let $D \subseteq K$ be the ring of integers in K and let $\alpha_1, \dots, \alpha_n \in D$ be a field basis for K/Q . Let $\Delta = \Delta(\alpha_1, \dots, \alpha_n)$ be the discriminant of this basis. Then $\Delta D \subseteq \mathcal{Z}\alpha_1 + \dots + \mathcal{Z}\alpha_n$.*

Proof. Let $w \in D$. We have $w = \sum r_i \alpha_i$ with $r_i \in Q$. Multiply both sides by α_j and take the trace. We find $Tr(w\alpha_j) = \sum r_i Tr(\alpha_i \alpha_j)$. The elements $Tr(w\alpha_j)$ and $Tr(\alpha_i \alpha_j)$ are all in \mathcal{Z} since they are traces of algebraic integers. Using Cramer's rule to solve for the r_i , we see that each r_i is an integer divided by Δ . The result follows. \square

Lemma 3.2.2. *The discriminant $\Delta = \Delta(1, \zeta_m, \dots, \zeta_m^{\phi(m)-1})$ divides $m^{\phi(m)}$.*

Proof. Differentiate both sides of $x^m - 1 = \Phi_m(x)g(x)$ to obtain $mx^{m-1} = \Phi'_m(x)g(x) + \Phi_m(x)g'(x)$. Substitute $x = \zeta_m$. The result is

$$m\zeta_m^{m-1} = \Phi'_m(\zeta_m)g(\zeta_m).$$

Now take the norm of both sides. On the left hand side we get:

$$N(m\zeta_m^{m-1}) = \prod_{i=1}^{\phi(m)} (m\zeta_m^{m-1})^{\sigma_i} = m^{\phi(m)} \prod_{i=1}^{\phi(m)} (\zeta_m^{m-1})^{\sigma_i} = m^{\phi(m)} N(\zeta_m)^{m-1}.$$

Using the factorization of $x^m - 1$ and induction we can show that $N(\zeta_m) = \pm 1$. Hence we get

$$N(m\zeta_m^{m-1}) = \pm m^{\phi(m)} = N(\Phi'_m(\zeta_m)g(\zeta_m)) = N(\Phi'_m(\zeta_m))N(g(\zeta_m)).$$

From this and Theorem 2.1.4 it follows that

$$\pm m^{\phi(m)} = \Delta N(g(\zeta_m)).$$

Since $1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}$ is a basis for $Q(\zeta_m)/Q$, $\Delta \neq 0$. Hence Δ divides $m^{\phi(m)}$. \square

Theorem 3.2.3. *Let $w \in D_m$. Then there is an element $\sum a_i \zeta_m^i \in \mathcal{Z}[\zeta_m]$ such that $w \equiv \sum a_i \zeta_m^i \pmod{(p)}$. (Recall that p is a prime not dividing m .)*

Proof. Let $\Delta = \Delta(1, \zeta_m, \dots, \zeta_m^{\phi(m)-1})$. By Lemma 3.2.2, p does not divide Δ . Thus there is a $\Delta' \in \mathcal{Z}$ such that $\Delta'\Delta \equiv 1 \pmod{(p)}$. Thus $w \equiv \Delta'\Delta w \pmod{(p)}$. By Lemma 3.2.1, $\Delta w \in \mathcal{Z}[\zeta_m]$. \square

Corollary 3.2.4. *Suppose p does not divide m and $n > 0$ is such that $p^n \equiv 1 \pmod{(m)}$. Then for $w \in D$ we have $w^{p^n} \equiv w \pmod{(p)}$.*

Proof. By the last theorem, $w \equiv \sum a_i \zeta_m^i$ with the $a_i \in \mathcal{Z}$. Since $a_i^p \equiv a_i \pmod{(p)}$ we must have $w^p \equiv \sum a_i \zeta_m^{p^i} \pmod{(p)}$. Repeating this process n times and using the fact that $p^n \equiv 1 \pmod{(m)}$ implies that $\zeta_m^{p^n} = \zeta_m$ yields the result. \square

Theorem 3.2.5. *If p is a prime that does not divide m , then every prime ideal P in D_m containing p is unramified.*

Proof. Assume P is ramified. Then $(p) \subseteq P^2$. Let w be an element of P not in P^2 , so $w^2 \in P^2$. By the above corollary $w^{p^n} \equiv w \pmod{(p)}$, implying that $w^{p^n} \equiv w \pmod{P^2}$. Since $p^n \geq 2$ it follows that $w \in P^2$, a contradiction. \square

Recall that for p a prime not dividing m the automorphism σ_p maps ζ_m to ζ_m^p .

Theorem 3.2.6. *For all $w \in D_m$ we have $\sigma_p w \equiv w^p \pmod{(p)}$.*

Proof. By Theorem 3.2.3 $w \equiv \sum a_i \zeta_m^i \pmod{(p)}$. Apply σ_p to both sides to obtain $\sigma_p w \equiv \sum a_i \zeta_m^{pi} \pmod{(p)}$. Since the $a_i \in \mathcal{Z}$ we have $\sum a_i \zeta_m^{pi} \equiv \sum a_i^p \zeta_m^i \equiv (\sum a_i \zeta_m^i)^p \pmod{(p)}$. Thus $\sigma_p w \equiv w^p \pmod{(p)}$ as asserted. \square

Corollary 3.2.7. *Let P be a prime ideal of D_m containing p . Then $\sigma_p(P) = P$.*

Proof. If $w \in P$, then $\sigma_p w \equiv w^p \equiv 0 \pmod{P}$, so $\sigma_p P \subseteq P$. Since $\sigma_p(P)$ is a maximal ideal, we have equality. \square

Theorem 3.2.8. *Let p be a prime not dividing m . Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{m}$. Then in $D_m \subseteq Q(\zeta_m)$*

$$(p) = P_1 P_2 \cdots P_g,$$

where each P_i has degree f and $g = \frac{\phi(m)}{f}$.

Proof. Since $Q(\zeta_m)/Q$ is a Galois extension, by Theorems 2.3.6 and 3.2.5 we have that $(p) = P_1 P_2 \cdots P_g$ where P_1, \dots, P_g are distinct, unramified primes, so $e = 1$. From $efg = \phi(m)$ the theorem follows. \square

Proof. (Alternative) By Theorem 2.2.21 we know that every prime ideal can be written as a product of prime ideals:

$$(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}.$$

Recall that $\sigma_p : \zeta_m \mapsto \zeta_m^p$. So $(\sigma_p)^f : \zeta_m \mapsto \zeta_m^{p^f}$. Since $p^f \equiv 1 \pmod{m}$, we get $(\sigma_p)^f(\zeta_m) = \zeta_m^{p^f} = \zeta_m$. As f is the smallest positive integer such that $p^f \equiv 1 \pmod{m}$, f is the smallest power of σ_p that sends ζ_m to itself. Hence f is the order of the automorphism σ_p . Therefore for all $w \in D_m$ we have $\sigma_p^f(w) = w$. Let $|D_m/P_1| = p^{f_1}$. Since D_m/P_1 is a finite field, we

have that for all nonzero $w \in D_m$, $w^{p^{f_1}-1} \equiv 1 \pmod{P_1}$, which implies that $w^{p^{f_1}} \equiv w \pmod{P_1}$. Furthermore we have that f_1 is the smallest positive integer with this property.

By Theorem 3.2.6 we have $w \equiv \sigma_p^f(w) \equiv w^{p^f} \pmod{P_1}$ for all $w \in D_m$. It follows that $f_1 \leq f$. But then by Theorem 3.1.5, $p^{f_1} \equiv 1 \pmod{m}$. Hence f divides f_1 , i.e., $f \leq f_1$. This shows that $f = f_1 = \text{degree of } P_1$. All the P_i have degree f . By theorem 3.2.5 all the P_i are unramified. From $efg = \phi(m)$ we conclude $g = \phi(m)/f$. \square

Corollary 3.2.9. *With the notation of the previous theorem, let P be one of the P_i . Define $G(P) = \{\sigma \in G : \sigma(P) = P\}$. Then $G(P)$ is a cyclic group of order f generated by σ_p . $G(P)$ is called the decomposition group of the prime ideal $P \subset D_m$.*

Proof. By Corollary 3.2.7 we know $\sigma_p \in G(P)$, so $\langle \sigma_p \rangle \subseteq G(P)$. By Theorem 2.3.5 we see that $g|G(P)| = \phi(m)$. Thus $|G(P)| = \phi(m)/g = f = |\langle \sigma_p \rangle|$. \square

Theorem 3.2.8 is a very satisfactory result on the decomposition of primes which do not divide m . There is also a general result that gives the decomposition of an arbitrary prime in a cyclotomic extension. For reference we state without proof the general result and then prove a special case that we need.

Theorem 3.2.10. *Let m' be a positive integer and let p be a prime. Write $m' = p^a m$ with $(m, p) = 1$ and $a \geq 0$. Put $f = |p|_m$, so $p^b \equiv 1 \pmod{m}$ if and only if f divides b . Then (p) factors in $D_{m'}$ as*

$$(p) = \prod_{i=1}^g P_i^{\phi(p^a)}$$

where $g = \phi(m)/f$ and the P_i are distinct prime ideals.

Proof. See Theorem 8.8 of H. B. Mann, *Algebraic Number Theory*. \square

We now prove the following important special case.

Theorem 3.2.11. *Let l be a prime in \mathcal{Z} . Then in D_l l ramifies completely. More precisely, put $L = (1 - \zeta_l)$. Then L is a prime ideal and $(l) = L^{(l-1)} = L^{\phi(l)}$. Moreover, L has degree 1.*

Proof. As in the proof of Theorem 3.1.5 we have $l = \prod(1 - \zeta_l^i)$, where the product is over all i with $1 \leq i \leq l - 1$.

Put $\zeta = \zeta_l$ and let $u_i = (1 - \zeta^i)/(1 - \zeta) = 1 + \zeta + \zeta^2 + \dots + \zeta^{i-1}$. We claim that u_i is a unit. Since $(l, i) = 1$ there is a $j \in \mathcal{Z}$ such that $ij \equiv 1 \pmod{l}$. Thus $u_i^{-1} = (1 - \zeta)/(1 - \zeta^i) = (1 - \zeta^{ij})/(1 - \zeta^i) = 1 + \zeta^i + \dots + (\zeta^i)^{j-1}$ is an algebraic integer, proving the claim.

It follows that $(l) = \prod(1 - \zeta^i) = (1 - \zeta)^{l-1} \prod u_i = L^{l-1}$. Using the relation $efg = \phi(l) = l - 1$, we see that L must be prime, $e = l - 1$, $g = 1$, and $f = 1$. \square

Theorem 3.2.12. *Let P be a prime ideal in D_m and set $P \cap \mathcal{Z} = p\mathcal{Z}$. If p is odd, then P is ramified if and only if $p|m$. If $p = 2$, then P is ramified if and only if $4|m$.*

Proof. By Theorem 3.2.5 we know that if p does not divide m , then P is unramified. Suppose p is odd and $p|m$. Then $Q(\zeta_p) \subseteq Q(\zeta_m)$. By Theorem 3.2.11 $pD_p = (1 - \zeta_p)^{p-1}$. Write $(1 - \zeta_p)D_m = P_1P_2 \cdots P_t$ where the P_i are, not necessarily distinct, prime ideals in D_m . Then $pD_m = (P_1P_2 \cdots P_t)^{p-1}$. Since $p - 1 > 1$, all the primes in D_m containing p are ramified.

Now suppose $p = 2$. If $2|m$ but 4 does not divide m , then $m = 2m_0$ with m_0 odd. In this case $-\zeta_{m_0}$ is a primitive m th root of unity, so $D_m = D_{m_0}$. Since 2 does not divide m_0 , P is unramified.

Finally, suppose $p = 2$ and $4|m$. Then $\zeta_4 = \sqrt{-1} = i \in D_m$. Since $(1 - i)^2 = -2i$, we see $2D_m = ((1 - i)D_m)^2$, and it follows as before that all the primes in D_m containing 2 are ramified. \square

Suppose p is a prime not dividing m . We need to know how p decomposes in the field $Q(\zeta_p, \zeta_m)$.

Lemma 3.2.13. *If $(m, n) = 1$, then $Q(\zeta_m, \zeta_n) = Q(\zeta_{mn})$.*

Proof. Clearly $Q(\zeta_m, \zeta_n) \subseteq Q(\zeta_{mn})$. On the other hand, since $(m, n) = 1$, there exist integers u and v such that $um + vn = 1$. Thus $\zeta_{mn} = \zeta_{mn}^{um} \zeta_{mn}^{vn} = \zeta_n^u \zeta_m^v \in Q(\zeta_m, \zeta_n)$. \square

In order to prove the final theorem of this section we need two lemmas, the first of which is quite general.

Let L/K be a Galois extension of fields, and assume L is Galois over Q . Denote the respective rings of algebraic integers by \mathcal{O}_L and \mathcal{O}_K . We wish to consider the factorization in the larger ring \mathcal{O}_L of the primes P from the

smaller ring \mathcal{O}_K . Since the ideal $P\mathcal{O}_L$ factors as a product of primes of \mathcal{O}_L , we know that P is contained in some prime ideal of \mathcal{O}_L .

Lemma 3.2.14. *Let P be a prime ideal in \mathcal{O}_K . If \bar{P} is a prime of \mathcal{O}_L , and $P \subset \bar{P}$, then $\bar{P} \cap \mathcal{O}_K = P$.*

Proof. Since $\bar{P} \cap \mathcal{O}_K$ is an ideal of \mathcal{O}_K containing P , and P is maximal, either $\bar{P} \cap \mathcal{O}_K = P$ or $\bar{P} \cap \mathcal{O}_K = \mathcal{O}_K$. If the latter were true, then $1 \in \bar{P}$, implying that $\bar{P} = \mathcal{O}_L$, which is clearly a contradiction. Hence $\bar{P} \cap \mathcal{O}_K = P$ as claimed. \square

From this lemma we conclude that two distinct primes in \mathcal{O}_K cannot lift to the same prime in \mathcal{O}_L , since if P and Q were two primes of \mathcal{O}_K contained in the prime \bar{P} of \mathcal{O}_L , then $P = \bar{P} \cap \mathcal{O}_K = Q$.

Now let p be a rational prime, $\{P_i\}_{i=1}^g$ the prime ideals in \mathcal{O}_K containing p , and \bar{P} any prime ideal of \mathcal{O}_L containing p .

Lemma 3.2.15. *There is an embedding $\mathcal{O}_K/P_i \hookrightarrow \mathcal{O}_L/\bar{P}$ for some $i \leq g$. In other words, up to an isomorphism, \mathcal{O}_K/P_i is a subfield of \mathcal{O}_L/\bar{P} .*

Proof. Consider the natural homomorphism $\mathcal{O}_L \rightarrow \mathcal{O}_L/\bar{P}$. Let ϕ denote the restriction of this homomorphism to \mathcal{O}_K . Since $\mathcal{O}_K/\ker\phi \cong \phi(\mathcal{O}_K)$, we can clearly embed $\mathcal{O}_K/\ker\phi \hookrightarrow \mathcal{O}_L/\bar{P}$. Now $\ker\phi = \bar{P} \cap \mathcal{O}_K$ is a prime ideal in \mathcal{O}_K that contains p , which is easily verified. Thus $\ker\phi = P_i$ for some $i \leq g$. Then, for this same i , there is an embedding $\mathcal{O}_K/P_i \hookrightarrow \mathcal{O}_L/\bar{P}$. \square

Theorem 3.2.16. *Let p be a prime not dividing m . Then*

$$pD_{pm} = (P_1P_2 \cdots P_g)^{p-1},$$

where the P_i are distinct prime ideals of degree f and $g = \phi(m)/f$. The integer f is the order of p modulo m .

Proof. Since $D_p \subseteq D_{pm}$ we see, as in the proof of Theorem 3.2.12 that all the ramification indices of primes in D_{pm} containing p are divisible by $p-1$. Thus (in a Galois extension all the e 's and all the f 's are the same):

$$pD_{pm} = (P_1P_2 \cdots P_{g'})^{e'(p-1)}, \quad (3.1)$$

where the P_i are distinct prime ideals of degree f' , say, and $e' \geq 1$ is some integer.

By Theorem 3.2.8

$$pD_m = P'_1 P'_2 \cdots P'_g,$$

where the P'_i are prime ideals in D_m of degree f and $g = \phi(m)/f$ and f is the order of p modulo m .

By considering the prime decomposition of $P'_i D_{pm}$ and comparing with Eq. 3.1 we see $f' \geq f$ and $g' \geq g$. (When we lift pD_m to pD_{pm} , each prime P'_i of D_m containing p lifts to at least one prime of D_{pm} containing p , and if $i \neq j$ then all of the primes lying above P_i are distinct from the primes lying above P_j . This gives us that $g \leq g'$.)

From Eq. 3.1 and Lemma 3.2.13 we see

$$(p-1)\phi(m) = \phi(pm) = e'(p-1)f'g' \geq e'(p-1)f \cdot \frac{\phi(m)}{f}.$$

It follows that $\phi(m) \geq e'\phi(m)$. Hence $e' = 1$ and all the inequalities are equalities, i.e., $f' = f$ and $g' = g = \phi(m)/f$. \square

In this section we have shown that if p is a prime not dividing m , then for each $w \in D_m$ there is an element $\alpha \in \mathcal{Z}[\zeta]$ such that $w \equiv \alpha \pmod{p}$. And we have shown that the discriminant Δ of $\{1, \zeta_m, \dots, \zeta_m^{\phi(m)-1}\}$ divides $m^{\phi(m)}$. In fact, much more is known to be true. An exact formula for Δ is known, and $\{1, \zeta_m, \dots, \zeta_m^{\phi(m)-1}\}$ is an integral basis for D_m , i.e., $D_m = \mathcal{Z}[\zeta_m]$. (See Ribenboim, Sect. 16.2.) However, what we have shown is enough to permit us to view each element $w \in D_m$ modulo some prime ideal \mathcal{P} of D_m containing p as an element of $\mathcal{Z}[\zeta_m]/\mathcal{P}$.

Chapter 4

Gauss Sums and the Stickelberger Relation

4.1 The Norm of an Ideal

Let K/Q be an algebraic number field, D the ring of integers in K , and A an ideal of D .

Definition: The *norm* $N(A)$ of the ideal A is defined to be the number of elements in D/A .

Throughout this chapter assume that an ideal is nonzero unless a specific exception is made.

Theorem 4.1.1. *If $A, B \subseteq D$ are ideals, then $N(AB) = N(A)N(B)$.*

Proof. If A and B are relatively prime, then $D/AB \cong D/A \oplus D/B$ (by Theorem 2.3.1), so the assertion is clear in this case.

Let $A = P_1^{a_1} P_2^{a_2} \cdots P_t^{a_t}$ be the prime decomposition of A . We claim that $N(A) = (N(P_1))^{a_1} (N(P_2))^{a_2} \cdots (N(P_t))^{a_t}$. On the basis of what we have seen so far it will be sufficient to prove that $N(P^a) = (N(P))^a$ for any prime ideal P . But this is just a reformulation of Theorem 2.3.2. In the general case decompose A and B into products of prime ideals, multiply, apply the above result and rearrange terms. The result follows. \square

Theorem 4.1.2. *Suppose K/Q is a Galois extension with group G . Then*

$$\prod_{\sigma \in G} \sigma(A) = (N(A)).$$

Proof. Since both sides are multiplicative in A , it suffices to prove the result when A is a prime ideal P . Let P_1, P_2, \dots, P_g be the distinct prime ideals in the set $\{\sigma(P) : \sigma \in G\}$. Then $|G| = g|G(P)|$ where $G(P) = \{\sigma \in G : \sigma(P) = P\}$. Since $efg = n = [K : Q] = |G|$ we see that $|G(P)| = ef$. Hence by Theorems 2.3.5 and 2.3.6 we have

$$\prod_{\sigma \in G} \sigma(P) = (P_1 P_2 \cdots P_g)^{ef} = (p)^f = (p^f), \text{ where } P_i \cap \mathcal{Z} = p\mathcal{Z}.$$

Since $N(P) = |D/P| = p^f$, this completes the proof. \square

Theorem 4.1.3. *Let K/Q be Galois with group G . Let $\alpha \in D$ and let $A = (\alpha)$ be the principal ideal generated by α . Let $N(\alpha)$ be the norm of α . Then $N(A) = |N(\alpha)|$.*

Proof. $(N(A)) = \prod \sigma(A) = \prod \sigma((\alpha)) = \prod (\sigma(\alpha)) = (\prod \sigma(\alpha)) = (N(\alpha))$. Thus $N(A)$ and $N(\alpha)$ differ by a unit. Since they are both in \mathcal{Z} and $N(A)$ by definition is positive, we have $N(A) = |N(\alpha)|$. \square

4.2 An Additive Character on F

A *multiplicative character* on a finite field F is a character χ from the multiplicative group F^* of the field to the multiplicative group K^* of some field K having sufficiently many roots of unity (often the group \mathcal{C}^*). We can extend this definition for nontrivial characters to all of F by defining $\chi(0) = 0$. Note however, that we put $\chi_0(0) = 1$. Throughout this chapter we assume that χ and λ are nontrivial multiplicative characters of order dividing m .

Similarly, an *additive character* on a finite field F is a character ψ on the additive group of F to the multiplicative group K^* of some field K (often the complex m th roots of unity).

Obviously the results of Section 1.1 apply to both types of characters.

Now suppose that p is a rational prime not dividing the positive integer m , and let P be a prime ideal of D_m containing p . Suppose D_m/P has order p^f and put $F \cong D_m/P$ where F is the Galois field with p^f elements. Here we know that f is the order of p modulo m . For $\alpha \in F$ we have already defined the trace of α to be

$$Tr(\alpha) = \sum_{i=0}^{f-1} \alpha^{p^i}.$$

Since F has characteristic p , it is easy to see that $(Tr(\alpha))^p = Tr(\alpha)$, so $Tr : F \rightarrow \mathcal{Z}/p\mathcal{Z}$. Define $\psi : F \rightarrow \mathcal{C}^*$ by

$$\psi : F \rightarrow Q(\zeta_p) : \alpha \mapsto \zeta_p^{Tr(\alpha)}.$$

Clearly the values of ψ are the various p th complex roots of 1, and ψ is an additive character. This is the primary additive character of interest in these notes.

Theorem 4.2.1. *Let $a \in \mathcal{Z}$. Then $\sum_{\alpha \in F} \psi(a\alpha) = \begin{cases} p^f, & \text{if } a \equiv 0 \pmod{p}; \\ 0, & \text{otherwise.} \end{cases}$*

Proof. Since $a^{p^j-1} \equiv 1 \pmod{p}$ we have that

$$\begin{aligned} Tr(a\alpha) &= a\alpha + a^p\alpha^p + \cdots + a^{p^{f-1}}\alpha^{p^{f-1}} = a(\alpha + a^{p-1}\alpha^p + \cdots + a^{p^{f-1}-1}\alpha^{p^{f-1}}) = \\ &= a(\alpha + \alpha^p + \cdots + \alpha^{p^{f-1}}) = aTr(\alpha). \end{aligned}$$

If $a \equiv 0 \pmod{p}$, then $a = pa'$, $a' \in \mathcal{Z}$. Thus

$$\begin{aligned} \sum_{\alpha \in F} \psi(a\alpha) &= \sum_{\alpha \in F} \zeta_p^{Tr(pa'\alpha)} = \sum_{\alpha \in F} \zeta_p^{pTr(a'\alpha)} = \\ &= \sum_{\alpha \in F} 1 = p^f. \end{aligned}$$

Suppose $a \not\equiv 0 \pmod{p}$. the mapping $Tr : F \rightarrow \mathcal{Z}/p\mathcal{Z}$ will send p^{f-1} elements of F to each $i \in \mathcal{Z}/p\mathcal{Z}$. Combining this and the fact that $a\alpha$ will run through the elements of F as α does, we can write

$$\sum_{\alpha \in F} \psi(a\alpha) = \sum_{\alpha \in F} \zeta_p^{Tr(a\alpha)} = p^{f-1} \sum_{i=0}^{p-1} \zeta_p^{ai} = p^{f-1} \frac{\zeta_p^{ap} - 1}{\zeta_p^a - 1} = 0.$$

□

4.3 The Power Residue Symbol

Let m be a positive integer and D_m be the ring of integers in $Q(\zeta_m)$. Let P be a prime ideal in D_m not containing m . Finally, let $q = p^f = N(P) = |D_m/P|$. By Theorem 3.1.5 we know that the cosets (modulo P) of $1, \zeta_m, \dots, \zeta_m^{m-1}$ are distinct and form a multiplicative subgroup of order m of D_m/P , so that m divides $p^f - 1$, i.e., $p^f \equiv 1 \pmod{m}$. (Actually, $f = |p|_m$.)

Theorem 4.3.1. *Let $\alpha \in D_m$, $\notin P$. Then there is an integer i , unique modulo m , such that*

$$\alpha^{\frac{q-1}{m}} \equiv \zeta_m^i \pmod{P}.$$

Proof. Since the multiplicative group of D_m/P has $q-1$ elements, we have $\alpha^{q-1} \equiv 1 \pmod{P}$. Since $\left(\alpha^{\frac{q-1}{m}}\right)^m = \alpha^{q-1} \equiv 1 \pmod{P}$, we have that the coset mod P of $\alpha^{\frac{q-1}{m}}$ is an m th root of unity in D_m/P . Hence $\alpha^{\frac{q-1}{m}} \equiv \zeta_m^j \pmod{P}$ for some j , $0 \leq j < m$. If $i \not\equiv j \pmod{m}$, then $\zeta_m^i \not\equiv \zeta_m^j \pmod{P}$, so j is unique modulo m . (See Theorem 3.1.5.) \square

Definition: For $\alpha \in D_m$ and P a prime ideal not containing m , define the m th power residue symbol $(\alpha/P)_m$ as follows:

- (a) $(\alpha/P)_m = 0$ if $\alpha \in P$;
- (b) If $\alpha \notin P$, then $(\alpha/P)_m$ is the unique m th root of unity (in D_m) such that

$$\alpha^{(N(P)-1)/m} \equiv (\alpha/P)_m \pmod{P}.$$

Theorem 4.3.2. *Under the hypotheses of the previous definition:*

- (a) $(\alpha/P)_m = 1$ iff $x^m \equiv \alpha \pmod{P}$ is solvable in D_m .
- (b) For all $\alpha \in D_m$, $\alpha^{(N(P)-1)/m} \equiv (\alpha/P)_m \pmod{P}$.
- (c) $(\alpha\beta/P)_m = (\alpha/P)_m(\beta/P)_m$.
- (d) If $\alpha \equiv \beta \pmod{P}$, then $(\alpha/P)_m = (\beta/P)_m$.
- (d) $\left(\frac{\zeta_m}{P}\right)_m = \zeta_m^{(N(P)-1)/m}$.

Proof. Choose $x \in D_m$ so that the coset $\bar{x} = x + P$ is a primitive element for D_m/P . Then $(x^a)^{\frac{q-1}{m}} \equiv 1 \pmod{P}$ iff $a \equiv 0 \pmod{m}$ iff $x^a \equiv y^m \pmod{P}$ is solvable for y . Hence $\alpha^{\frac{q-1}{m}} \equiv 1 \pmod{P}$ iff $\alpha \equiv y^m \pmod{P}$ is solvable for $y \in D_m$. This proves (a). The remaining parts are similarly easy. \square

We now define the multiplicative character χ_P on the field $F \cong D_m/P$ of order $q = p^f$. Let $0 \neq t \in F$ and let $\gamma \in D_m$ such that $\bar{\gamma} = t$, where $\bar{\gamma}$ is the coset of P containing γ . Define

$$\chi_P(t) = \left(\frac{\gamma}{P}\right)_m^{-1} = \overline{\left(\frac{\gamma}{P}\right)_m}.$$

4.4 Some Special Gauss and Jacobi Sums

For a nontrivial multiplicative character χ , a fixed element $a \in F$ and the special additive character ψ defined in Section 4.2,

$$g(\chi, \psi, a) = \sum_{\alpha \in F} \chi(\alpha) \psi(a\alpha) \in F.$$

This is a special kind of sum known as a *Gauss sum*.

Theorem 4.4.1. *If $a \neq 0$, then $g(\chi, \psi, a) = \chi(a^{-1})g(\chi, \psi, 1)$. If $a = 0$, then $g(\chi, \psi, 0) = 0$.*

Proof. First suppose that $a \neq 0$. Then

$$\chi(a)g(\chi, \psi, a) = \chi(a) \sum_{\alpha \in F} \chi(\alpha) \psi(a\alpha) = \sum_{\alpha \in F} \chi(a\alpha) \psi(a\alpha).$$

Since $a\alpha$ runs through all of the elements of F , we have

$$\chi(a)g(\chi, \psi, a) = \sum_{\alpha \in F} \chi(\alpha) \psi(\alpha) = g(\chi, \psi, 1).$$

Since $\chi(\alpha)^{-1} = \overline{\chi(\alpha)} = \chi(\alpha^{-1})$ we get

$$g(\chi, \psi, a) = \chi(a^{-1})g(\chi, \psi, 1).$$

If $a = 0$, then $g(\chi, \psi, 0) = \sum_{\alpha \in F} \chi(\alpha) = 0$ by Corollary 1.1.5. □

If we put $a = 1$ above and χ is any multiplicative character, define

$$g(\chi) := \sum_{\alpha \in F_q} \chi(\alpha) \psi(\alpha).$$

When $\chi = \chi_P$, define

$$g(P) := g(\chi_P) := g(\chi_P, \psi, 1) \text{ and } \Phi(P) := g(P)^m.$$

Here: p does not divide m , $f = |p|_m$, $q = p^f$ so m divides $q - 1$.

The goal of this chapter is to find the prime decomposition of $\Phi(P)$ in D_m .

Theorem 4.4.2. *This theorem is a standard result in the theory of Gauss sums.*

(i) $g(P) \in Q(\zeta_m, \zeta_p) = Q(\zeta_{pm})$.

(ii) If χ is any multiplicative character different from χ_0 , then $g(\chi)\overline{g(\chi)} = q$.

(iii) As a special case we have $|g(P)|^2 = q$.

Proof. Start with

$$g(P) = \sum_{\alpha \in F} \chi_P(\alpha) \psi(\alpha) = \sum_{\alpha \in F} \overline{\left(\frac{\alpha}{P}\right)_m} \zeta_p^{Tr(\alpha)} = \sum_{\alpha \in F} \left(\frac{\alpha}{P}\right)_m \zeta_p^{-Tr(\alpha)}.$$

So each term of the sum looks like $\zeta_m^j \zeta_p^{-Tr(\alpha)} \in Q(\zeta_m, \zeta_p)$ (where j is the unique integer defined in Theorem 4.3.1) or is equal to 0 if $\alpha \in P$. This proves part (i).

Note: In the following proof of part (iii) if χ_P is replaced everywhere with just χ , then a proof of part (ii) is given.

To show $|g(P)|^2 = q$ we will evaluate $\sum_{a \in F} g(\chi_P, \psi, a) \overline{g(\chi_P, \psi, a)}$ in two different ways. If $a \neq 0$, then by Theorem 4.4.1 we have

$$\overline{g(\chi_P, \psi, a)} = \chi_P(a) \overline{g(\chi_P, \psi, 1)} = \chi_P(a) \overline{g(\chi_P)}$$

and $g(\chi_P, \psi, a) = \chi_P(a^{-1})g(\chi_P)$. Therefore we have

$$g(\chi_P, \psi, a) \overline{g(\chi_P, \psi, a)} = \chi_P(a) \chi_P(a^{-1}) g(\chi_P) \overline{g(\chi_P)} = |g(\chi_P)|^2.$$

Since $g(\chi_P, \psi, 0) = 0$, we obtain

$$\begin{aligned} \sum_{a \in F} g(\chi_P, \psi, a) \overline{g(\chi_P, \psi, a)} &= \sum_{a \in F^*} g(\chi_P, \psi, a) \overline{g(\chi_P, \psi, a)} = \\ &= \sum_{a \in F^*} |g(\chi_P)|^2 = \sum_{a \in F^*} |g(P)|^2 = (q-1)|g(P)|^2. \end{aligned}$$

On the other hand we have

$$\begin{aligned} g(\chi_P, \psi, a) \overline{g(\chi_P, \psi, a)} &= \sum_{\alpha \in F} \chi_P(\alpha) \psi(a\alpha) \overline{\sum_{\beta \in F} \chi_P(\beta) \psi(a\beta)} = \\ \sum_{\alpha, \beta \in F} \overline{\chi_P(\beta) \psi(a\beta)} \chi_P(\alpha) \psi(a\alpha) &= \sum_{\alpha, \beta \in F} \chi_P(\alpha) \overline{\chi_P(\beta)} \psi(a\alpha) \psi(-a\beta) = \end{aligned}$$

$$\begin{aligned}
&= \sum_{\alpha, \beta \in F} \chi_P(\alpha\beta^{-1})\psi(a(\alpha - \beta)) = \\
&= q + \sum_{\alpha \neq \beta} \chi_P(\alpha\beta^{-1})\psi(a(\alpha - \beta)).
\end{aligned}$$

Now summing over all nonzero $a \in F$ we get

$$\begin{aligned}
&\sum_{a \in F^*} \left(q + \sum_{\alpha \neq \beta} \chi_P(\alpha\beta^{-1})\psi(a(\alpha - \beta)) \right) = \\
&= (q-1)q + \sum_{\alpha \in F^*} \sum_{\alpha \neq \beta} \chi_P(\alpha\beta^{-1})\psi(a(\alpha - \beta)) = \\
&= (q-1)q + \sum_{\alpha \neq \beta} \sum_{a \in F^*} \chi_P(\alpha\beta^{-1})\psi(a(\alpha - \beta)).
\end{aligned}$$

Fixing α and β (with $\alpha \neq \beta$) and applying Theorem 4.2.1 we get

$$\sum_{a \in F^*} \chi_P(\alpha\beta^{-1})\psi(a(\alpha - \beta)) = \chi_P(\alpha\beta^{-1}) \sum_{a \in F^*} \psi(a(\alpha - \beta)) = 0.$$

So now we have

$$(q-1)|g(P)|^2 = \sum_{a \in F^*} g(\chi_P, \psi, a) \overline{g(\chi_P, \psi, a)} = (q-1)q$$

and thus $(q-1)|g(P)|^2 = (q-1)q$. □

Lemma 4.4.3.

$$g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}.$$

Proof.

$$\begin{aligned}
\overline{g(\chi)} &= \overline{\sum_{\alpha \in F} \chi(\alpha)\psi(\alpha)} = \sum_{\alpha \in F} \overline{\chi(\alpha)\psi(\alpha)} = \sum_{\alpha \in F} \overline{\chi(-1)\chi(-\alpha)\psi(-\alpha)} = \\
&= \overline{\chi(-1)} \sum_{\alpha \in F} \overline{\chi(-\alpha)\psi(-\alpha)}.
\end{aligned}$$

However, since $\chi(-1) = \pm 1$, multiplying both sides by $\chi(-1)$ we get

$$\chi(-1)\overline{g(\chi)} = \sum_{\alpha \in F} \overline{\chi(\alpha)\psi(\alpha)} = g(\overline{\chi}).$$

□

If χ and λ are two multiplicative characters on F we define their *Jacobi sum* to be

$$J(\chi, \lambda) = \sum_{\alpha+\beta=1} \chi(\alpha)\lambda(\beta), \text{ where } \alpha, \beta \in F.$$

Theorem 4.4.4. *If χ , λ , and $\chi\lambda$ are nontrivial, then*

$$g(\chi)g(\lambda) = g(\chi\lambda)J(\chi, \lambda),$$

and as an immediate corollary of this and Theorem 4.4.2

$$J(\chi, \lambda)\overline{J(\chi, \lambda)} = q.$$

Proof. First notice that

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_{\alpha \in F} \chi(\alpha)\psi(\alpha) \right) \left(\sum_{\beta \in F} \lambda(\beta)\psi(\beta) \right) = \\ &= \sum_{\alpha, \beta \in F} \chi(\alpha)\lambda(\beta)\psi(\alpha + \beta) = \sum_{\gamma \in F} \left(\sum_{\alpha+\beta=\gamma} \chi(\alpha)\lambda(\beta)\psi(\gamma) \right) = \\ &= \sum_{\gamma \in F} \left(\sum_{\alpha+\beta=\gamma} \chi(\alpha)\lambda(\beta) \right) \psi(\gamma). \end{aligned}$$

If $\gamma = 0$ we have $\sum_{\alpha+\beta=0} \chi(\alpha)\lambda(\beta) =$

$$\sum_{\alpha \in F} \chi(\alpha)\lambda(-\alpha) = \sum_{\alpha \in F} \chi(\alpha)\lambda(-1)\lambda(\alpha) = \lambda(-1) \sum_{\alpha \in F} \chi\lambda(\alpha) = 0.$$

If $\gamma \neq 0$, then define $\alpha', \beta' \in F$ by $\alpha'\gamma = \alpha$ and $\beta'\gamma = \beta$. So $\alpha + \beta = \gamma$ is equivalent to $\alpha' + \beta' = 1$. Thus

$$\sum_{\alpha+\beta=\gamma} \chi(\alpha)\lambda(\beta) = \chi\lambda(\gamma) \sum_{\alpha'+\beta'=1} \chi(\alpha')\lambda(\beta') = \chi\lambda(\gamma)J(\chi, \lambda).$$

Therefore we have

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_{\gamma \in F} (\chi\lambda(\gamma)J(\chi, \lambda))\psi(\gamma) = \\ &= J(\chi, \lambda) \sum_{\gamma \in F} \chi\lambda(\gamma)\psi(\gamma) = J(\chi, \lambda)g(\chi\lambda). \end{aligned}$$

□

Theorem 4.4.5.

$$\Phi(P) = \chi_P(-1)q \prod_{i=1}^{m-1} J(\chi_P, \chi_P^i) \in Q(\zeta_m).$$

Proof. By the preceding theorem we have

$$g(\chi_P)^2 = g((\chi_P)^2)J(\chi_P, \chi_P).$$

Multiplying both sides of the equation by $g(\chi_P)$ we get

$$g(\chi_P)^3 = g(\chi_P)g((\chi_P)^2)J(\chi_P, \chi_P) = g((\chi_P)^3)J(\chi_P, (\chi_P)^2)J(\chi_P, \chi_P).$$

Continuing with this process we eventually get

$$g(\chi_P)^{m-1} = g((\chi_P)^{m-1}) \prod_{i=1}^{m-1} J(\chi_P, (\chi_P)^i).$$

Multiplying once more by $g(\chi_P)$ we get

$$\begin{aligned} \Phi(P) &= g(\chi_P)^m = g(\chi_P)g((\chi_P)^{m-1}) \prod_{i=1}^{m-1} J(\chi_P, (\chi_P)^i) = \\ &= g(\chi_P)g((\chi_P)^{-1}) \prod_{i=1}^{m-1} J(\chi_P, (\chi_P)^i). \end{aligned}$$

Now use $g(\chi_P)g((\chi_P)^{-1}) = g(\chi_P)g(\overline{\chi_P})$

$$= g(\chi_P)\chi_P(-1)\overline{g(\chi_P)} = \chi_P(-1)|g(\chi_P)|^2 = \chi_P(-1)q$$

to write

$$\Phi(P) = \chi_P(-1)q \prod_{i=1}^{m-1} J(\chi_P, (\chi_P)^i).$$

It is also easy to see that all individual terms of $\Phi(P)$ are in $Q(\zeta_m)$. \square

We emphasize the fact that the reason for doing the calculations of the preceding theorem was precisely to show that $\Phi(P) \in Q(\zeta_m)$. Moreover, χ_P could have been replaced by any multiplicative character of order dividing m .

4.5 Factoring Ideals in D_m

In this section we assume throughout that p is a prime not dividing m and that $f = |p|_m$. Put $q = p^f$ so $m|(q-1)$. It is also clear that $f = |p|_{q-1}$. We will now be working with the fields $Q \subseteq Q(\zeta_m) \subseteq Q(\zeta_{q-1}) \subseteq Q(\zeta_{p(q-1)})$ with respective rings of integers $\mathcal{Z} \subseteq D_m \subseteq D_{q-1} \subseteq D_{p(q-1)}$ and prime ideals $(p) \subset P \subseteq B \subset \mathcal{P}$. Also put $\lambda_p = 1 - \zeta_p$ and recall that in D_p the principal ideal (p) ramifies completely: $(p) = (\lambda_p)^{p-1}$ and (λ_p) is prime in D_p . The following diagram will be handy.

$$\begin{array}{ccccccc}
 (\lambda_p)^{(p-1)} = (\mathcal{P}_1 \cdots \mathcal{P}_h)^{(p-1)} & \mathcal{P} & \subset & D_{(q-1)p} & \rightarrow & D_{(q-1)p}/\mathcal{P} \\
 & | & & | & & | \\
 (p) = \mathcal{B}_1 \cdots \mathcal{B}_h & \mathcal{B} & \subset & D_{q-1} & \rightarrow & D_{q-1}/\mathcal{B} \\
 & | & & | & & | \\
 (p) = P_1 \cdots P_g & P & \subset & D_m & \rightarrow & D_m/P \\
 & | & & | & & | \\
 & (p) & \subset & \mathcal{Z} & \rightarrow & \mathcal{Z}/p\mathcal{Z}
 \end{array}$$

Lemma 4.5.1. *Recall that from Theorem 3.2.16 (with m of that theorem replaced by $q-1$) we have*

$$pD_{p(q-1)} = (\mathcal{P}_1 \cdots \mathcal{P}_h)^{p-1}, \quad h = \frac{\phi(q-1)}{f}$$

Then:

- (i) $\text{ord}_{\mathcal{P}}(pD_{p(q-1)}) = p-1$.
- (ii) $\text{ord}_{\mathcal{P}}(\lambda_p) = 1$.
- (iii) $\text{ord}_{\mathcal{P}}(P) = p-1$.

Proof. Part (i) is clear. Factoring $pD_{p(q-1)}$ differently we get

$$\begin{aligned}
 (\mathcal{P}_1 \cdots \mathcal{P}_h)^{(p-1)} &= (pD_p)D_{p(q-1)} = (\lambda_p)^{p-1}D_{p(q-1)} = \\
 &= (\mathcal{P}_1 \cdots \mathcal{P}_h)^{p-1}, \text{ where, say, } \mathcal{P} = \mathcal{P}_1,
 \end{aligned}$$

and therefore $\lambda_p D_{p(q-1)} = \mathcal{P}_1 \cdots \mathcal{P}_h$. This proves (ii). To prove (iii), first note that the only ramification that takes place does so when lifting from $D_{(q-1)}$ to $D_{p(q-1)}$. In D_m we have $(p)D_m = P_1 \cdots P_g$ where P_1, \dots, P_g are the distinct prime ideals in D_m lying over (p) , and $g = \frac{\phi(m)}{f}$. Then in $D_{(q-1)}$ (p) splits into the product of distinct primes $(p)D_{(q-1)} = \mathcal{B}_1 \cdots \mathcal{B}_h$, where each

P_i splits in $D_{(q-1)}$ into the product of h/g distinct primes. Here $h = \frac{\phi(q-1)}{f}$. Then in $D_{p(q-1)}$ each \mathcal{B}_i splits into the $p-1 = \phi(p)$ th power of a single prime \mathcal{P}_i . So each prime ideal of $D_{p(q-1)}$ lying over (p) in \mathcal{Z} is raised to the $(p-1)$ th power in the factorization of (p) . This proves (iii). \square

Lemma 4.5.2. $D_m/P \cong D_{q-1}/\mathcal{B}$.

Proof. This really just the observation that $|p|_m = f = |p|_{q-1}$, along with Theorem 3.2.8. \square

By Theorem 3.1.5 we know that the elements $1, \zeta_{q-1}, \dots, \zeta_{q-1}^{q-2}$ have distinct images in D_{q-1}/\mathcal{B} , so that in fact these images are precisely all the nonzero elements of the field D_{q-1}/\mathcal{B} . The following definition imitates the definition of the m th power residue symbol.

Definition: For $\alpha \in D_{q-1}$ define

(a) $\left(\frac{\alpha}{\mathcal{B}}\right) = 0 \in D_{q-1}$ if $\alpha \in \mathcal{B}$.

(b) If $\alpha \notin \mathcal{B}$, $\left(\frac{\alpha}{\mathcal{B}}\right)$ is the unique $(q-1)$ -st root of unity in D_{q-1} such that $\alpha \equiv \left(\frac{\alpha}{\mathcal{B}}\right) \pmod{\mathcal{B}}$.

It is easy to see that

$$\left(\frac{\alpha\beta}{\mathcal{B}}\right) = \left(\frac{\alpha}{\mathcal{B}}\right) \left(\frac{\beta}{\mathcal{B}}\right), \quad (4.1)$$

and

$$\alpha \equiv \beta \pmod{\mathcal{B}} \text{ implies that } \left(\frac{\alpha}{\mathcal{B}}\right) = \left(\frac{\beta}{\mathcal{B}}\right). \quad (4.2)$$

Lemma 4.5.3. If $\alpha \in D_m$, $\left(\frac{\alpha}{\mathcal{B}}\right)^{(q-1)/m} = \left(\frac{\alpha}{P}\right)_m$.

Proof. This is really an immediate consequence of the definitions. \square

4.6 The Teichmüller Character

Using the same notation as in the last section, choose a prime ideal \mathcal{B} in D_{q-1} lying over (p) . The *Teichmüller character* is a multiplicative character $w_{\mathcal{B}}$ on $F_q \cong D_{q-1}/\mathcal{B}$ defined as follows. For each $t \in F_q^*$, let γ be any element of D_{q-1} for which $\bar{\gamma} = t$. Then $w_{\mathcal{B}}(t) = \left(\frac{\gamma}{\mathcal{B}}\right)$. The proof that $w_{\mathcal{B}}$ is well-defined and is a multiplicative character follows immediately from the properties of the symbol $\left(\frac{\gamma}{\mathcal{B}}\right)$.

Lemma 4.6.1.

$$w_{\mathcal{B}}(\bar{\zeta}_{q-1}^i) = \zeta_{q-1}^i.$$

Proof. This is rather immediate from the fact that by definition $\left(\frac{\bar{\zeta}_{q-1}}{\mathcal{B}}\right) = \zeta_{q-1}$. \square

Consequently $w_{\mathcal{B}}$ has order $q - 1$ and must generate the entire group of multiplicative characters on F_q .

Lemma 4.6.2. *Let $t \in F_q$. Then $w_{\mathcal{B}}^{-\left(\frac{q-1}{m}\right)}(t) = \chi_P(t)$.*

Proof. Let $t \in F_q \cong D_{q-1}/\mathcal{B}$. If $t = \bar{\gamma} \pmod{P}$, $\gamma \in D_m$, then since $P \subset \mathcal{B}$, $t = \bar{\gamma} \pmod{\mathcal{B}}$. (Alternatively, we have already noted that $D_m/P \cong D_{q-1}/\mathcal{B}$.) Furthermore, since the cosets of $1, \zeta_{q-1}, \dots, \zeta_{q-1}^{q-2} \pmod{\mathcal{B}}$ are all the distinct elements of F_q^* , there must be a unique ζ_{q-1}^i such that $\gamma \equiv \zeta_{q-1}^i \pmod{\mathcal{B}}$. Then

$$w_{\mathcal{B}}^{-\left(\frac{q-1}{m}\right)}(t) = \left(\frac{\gamma}{\mathcal{B}}\right)^{-\left(\frac{q-1}{m}\right)}$$

which is an m th root of unity and therefore in D_m . Then

$$\begin{aligned} \chi_P(t) &= \left(\frac{\gamma}{P}\right)_m^{-1} \quad (\text{by definition of } \chi_P - \text{ see Thm.4.3.2}) \\ &= \gamma^{-\left(\frac{q-1}{m}\right)} \pmod{P} \quad (\text{by definition of } (\)_m) \\ &\equiv (\zeta_{q-1}^i)^{-\left(\frac{q-1}{m}\right)} \pmod{\mathcal{B}}. \end{aligned}$$

Hence $\chi_P(t) = (\zeta_{q-1}^i)^{-\left(\frac{q-1}{m}\right)} = w_{\mathcal{B}}^{-\left(\frac{q-1}{m}\right)}(t)$. \square

4.7 Stickelberger's Theorem at Last

In this section we will let w denote the Teichmüller character $w_{\mathcal{B}}$.

Let a be a positive rational integer and define

$$g_a = g(w^{-a}) = \sum_{\alpha \in F_q} w(\alpha)^{-a} \psi(\alpha).$$

Lemma 4.7.1. *Define $\tilde{s}(a) = \text{ord}_{\mathcal{P}}(g_a)$. Then we have the following:*

- (i) $\tilde{s}(a+b) \leq \tilde{s}(a) + \tilde{s}(b)$, $1 \leq a, b, a+b < q-1$.
- (ii) $\tilde{s}(a+b) \equiv \tilde{s}(a) + \tilde{s}(b) \pmod{p-1}$.
- (iii) $\tilde{s}(pa) = \tilde{s}(a)$.

Proof. Applying Theorem 4.4.4 we get

$$\begin{aligned} g_a g_b &= g(w^{-a})g(w^{-b}) = g(w^{-a}w^{-b})J(w^{-a}, w^{-b}) = \\ &= g(w^{-a-b})J(w^{-a}, w^{-b}) = g_{a+b}J(w^{-a}, w^{-b}). \end{aligned}$$

Hence $\text{ord}_{\mathcal{P}}(g_a g_b) = \text{ord}_{\mathcal{P}}(g_{a+b}J(w^{-a}, w^{-b}))$. So we have

$$\text{ord}_{\mathcal{P}}(g_a) + \text{ord}_{\mathcal{P}}(g_b) = \text{ord}_{\mathcal{P}}(g_{a+b}) + \text{ord}_{\mathcal{P}}(J(w^{-a}, w^{-b})) \geq \text{ord}_{\mathcal{P}}(g_{a+b}),$$

and thus $\tilde{s}(a+b) \leq \tilde{s}(a) + \tilde{s}(b)$, proving part (i).

Note that $J(w^{-a}, w^{-b}) = \sum_{\alpha+\beta=1} w(\alpha)^{-a}w(\beta)^{-b}$, which is in $Q(\zeta_{q-1})$. It then follows from the fact that $\mathcal{B}D_{p(q-1)} = \mathcal{P}^{p-1}$ that $p-1$ divides $\text{ord}_{\mathcal{P}}J(w^{-a}, w^{-b})$. Then since $g(w^{-a})g(w^{-b}) = g(w^{-(a+b)})J(w^{-a}, w^{-b})$, we see that part (ii) holds. For part (iii), recall that $\alpha \mapsto \alpha^p$ is an automorphism of F_q . Then $\psi(\alpha^p) = \zeta_p^{\text{Tr}(\alpha^p)} = \zeta_p^{\text{Tr}(\alpha)} = \psi(\alpha)$. Then $g_{pa} = \sum_{\alpha \in F_q} w(\alpha)^{-pa} \psi(\alpha) = \sum_{\alpha \in F_q} w(\alpha^p)^{-a} \psi(\alpha^p) = g_a$, from which it follows that $\tilde{s}(pa) = \tilde{s}(a)$. \square

This next theorem is also due to Stickelberger and is the last result in this chapter that we really need to proceed on into the next chapter. The remaining results of this chapter are included just for completeness.

Theorem 4.7.2. *For $1 \leq a \leq q-1$ we have $\tilde{s}(a) = \text{ord}_{\mathcal{P}}(g_a) = S(a)$.*

Proof. Clearly $S(1) = 1$, so we start by showing $\tilde{s}(1) = 1$. Recall

$$g_1 = \sum_{t \in F_q} w(t)^{-1} \zeta_p^{\text{Tr}(t)}.$$

Also, recall $\zeta_p = 1 - \lambda_p$. Now we use Lemma 4.6.1 to convert the expression for g_1 into a sum over the powers of ζ_{q-1} . Let m_i be a positive integer such that $m_i \equiv \text{Tr}(\zeta_{q-1}^i) \pmod{p}$. Then

$$g_1 = \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (1 - \lambda_p)^{m_i}.$$

Using the binomial theorem we see that $(1 - \lambda_p)^{m_i} \equiv 1 - m_i \lambda_p \pmod{\mathcal{P}^2}$ (since $(\lambda_p)^j \in \mathcal{P}^j \subset \mathcal{P}^2$), implying

$$g_1 \equiv \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} - \sum_{i=0}^{q-2} m_i \zeta_{q-1}^{-i} \lambda_p \pmod{\mathcal{P}^2}.$$

The first sum is just the sum of all the $(q-1)$ -th roots of unity which is zero. For the second sum, note that

$$m_i \equiv (\zeta_{q-1}^i + \zeta_{q-1}^{pi} + \cdots + \zeta_{q-1}^{(p^{f-1})i}) \pmod{\mathcal{P}^2}.$$

Substituting this in above we find

$$g_1 \equiv - \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (\zeta_{q-1}^i + \zeta_{q-1}^{pi} + \cdots + \zeta_{q-1}^{(p^{f-1})i}) \lambda_p \pmod{\mathcal{P}^2}.$$

All the sums $\sum_{i=0}^{q-2} \zeta_{q-1}^{(p^j-1)i}$ for $j = 1, 2, \dots, f-1$ are zero, while $j = 0$ gives

$$g_1 \equiv - \sum_{i=0}^{q-2} \zeta_{q-1}^0 \lambda_p = -(q-1)\lambda_p \equiv \lambda_p \pmod{\mathcal{P}^2}.$$

By Lemma 4.5.1 part (ii) we have that $\text{ord}_{\mathcal{P}}(g_1) = 1$, i.e., $\tilde{s}(1) = 1$. Now suppose $\tilde{s}(a) = a$ for $1 \leq a < n \leq p-1$. Applying Lemma 4.7.1 along with the induction hypothesis we have $\tilde{s}(n) \leq \tilde{s}(n-1) + \tilde{s}(1) = n-1+1 = n$ and $\tilde{s}(n) \equiv \tilde{s}(n-1) + \tilde{s}(1) = n \pmod{p-1}$. Hence $\tilde{s}(n) = n$.

Now for $1 \leq a \leq q-2$ we have $a = \sum_{i=0}^{f-1} a_i p^i$, $0 \leq a_i < p$. Applying Lemma 4.7.1 again we have

$$\tilde{s}(a) = \tilde{s} \left(\sum_{i=0}^{f-1} a_i p^i \right) \leq \sum_{i=0}^{f-1} \tilde{s}(a_i p^i) = \sum_{i=0}^{f-1} \tilde{s}(a_i) = \sum_{i=0}^{f-1} a_i = S(a).$$

We now have $\tilde{s}(a) \leq S(a)$ for all a in the range under consideration. To prove the theorem it will be enough in light of Lemma 1.5.3 to show that

$$\sum_{a=1}^{q-2} \tilde{s}(a) = \frac{f(p-1)(q-2)}{2}.$$

Recall that in general for Gauss sums we have the relation $g(\chi^{-1}) = \chi(-1)\overline{g(\chi)}$. Thus

$$\begin{aligned} g_a g_{q-1-a} &= g(w^{-a})g(w^{a+1-q}) = \\ &g((w^a)^{-1})g(w^{a+1-q}) = w^a(-1)\overline{g(w^a)}g(w^{a+1-q}). \end{aligned}$$

Also note that $w^{a+1-q} = w^{-1(q-1-a)} = (w^{-1})^{-a}$, implying

$$g_a g_{q-1-a} = w^a(-1)\overline{g(w^a)}g(w^a) = w^a(-1)|g(w^a)|^2 = w^a(-1)q = w^a(-1)p^f.$$

So we have

$$\tilde{s}(a) + \tilde{s}(q-1-a) = \text{ord}_{\mathcal{P}} g_a g_{q-1-a} = \text{ord}_{\mathcal{P}}(w^a(-1)p^f).$$

Since $w(-1) = \pm 1$, $w^a(-1)$ contributes nothing. We have that

$$(p)^f D_{p(q-1)} = (\mathcal{P}_1 \cdots \mathcal{P}_h)^{f(p-1)},$$

so $\tilde{s}(a) + \tilde{s}(q-1-a) = f(p-1)$. As a runs through $1, 2, \dots, q-2$, $q-1-a$ also runs through $q-1, q-1, \dots, 1$, which gives

$$\begin{aligned} \sum_{a=1}^{q-2} (\tilde{s}(a) + \tilde{s}(q-1-a)) &= \sum_{a=1}^{q-2} 2\tilde{s}(a) = \\ &= 2 \sum_{a=1}^{q-2} \tilde{s}(a) = \sum_{a=1}^{q-2} f(p-1) = f(p-1)(q-2). \end{aligned}$$

It now follows that

$$\sum_{a=1}^{q-2} \tilde{s}(a) = \frac{f(p-1)(q-2)}{2} = \sum_{a=1}^{q-2} S(a).$$

Then since $\tilde{s}(a) \leq S(a)$ for all a we have $\tilde{s}(a) = S(a)$ for $1 \leq a < q-1$.

Finally, notice that $g_0 = \sum_{\alpha \in F_q} w^{-(q-1)}(\alpha)\psi(\alpha) = \sum_{\alpha \in F_q} \psi(\alpha) = 0$, so $\tilde{s}(0) = 0$, so equality also holds when $a = q-1$. \square

Corollary 4.7.3. $\text{ord}_{\mathcal{P}}(\Phi(P)) = \frac{m}{p-1} S\left(\frac{q-1}{m}\right)$.

Proof. Note that by Theorem 4.4.2(iii) any prime ideal of D_m dividing $\Phi(P)$ lies over $p \in Z$. Let $\Phi(P) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$ be the prime factorization of $\Phi(P)$. By part (iii) of Lemma 4.5.1 we get

$$\Phi(P) = (\mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g})^{p-1},$$

so $\text{ord}_{P_i}(\Phi(P)) = (p-1)\text{ord}_{P_i}(\mathcal{P}_i^{e_i})$. Recall that $\Phi(P) = g(P)^m$, so $\text{ord}_{\mathcal{P}}(\Phi(P)) = m \cdot \text{ord}_{\mathcal{P}}(g(P))$.

We will now show that $g(P)$, defined in Section 4.4, is equal to g_a for $a = (q-1)/m$. Recall that

$$g_{\frac{q-1}{m}} = \sum_{\alpha \in F_q} w^{-\left(\frac{q-1}{m}\right)}(\alpha) \psi(\alpha)$$

and

$$g(P) = \sum_{\alpha \in F_q} \chi_P(\alpha) \psi(\alpha).$$

By Lemma 4.6.2 we have $\chi_P(t) = w^{-\left(\frac{q-1}{m}\right)}(t)$, and hence $g(P) = g_{\frac{q-1}{m}}$. If we now apply Theorem 4.7.2 and the definition of \tilde{s} we get $\text{ord}_{\mathcal{P}}(g_{\frac{q-1}{m}}) = S\left(\frac{q-1}{m}\right)$, which implies $\text{ord}_{\mathcal{P}}(\Phi(P)) = m \cdot \text{ord}_{\mathcal{P}}(g_{\frac{q-1}{m}}) = mS\left(\frac{q-1}{m}\right)$. This implies $(p-1) \cdot \text{ord}_{\mathcal{P}}(\Phi(P)) = m \cdot S\left(\frac{q-1}{m}\right)$, from which the Corollary follows. \square

Recall that for each $a \in \mathcal{Z}$ with $(a, m) = 1$, there is an automorphism σ_a of $Q(\zeta_m)$ mapping ζ_m to ζ_m^a . Moreover, if P' is another prime ideal of D_m containing p , then there is an automorphism σ_t of $Q(\zeta_m)$ such that $P' = \sigma_t^{-1}(P)$. So for $1 \leq t < m$ with $(t, m) = 1$ we will define $P_t = \sigma_t^{-1}P$.

Lemma 4.7.4. $\text{ord}_{P_t}(\Phi(P)) = \frac{m}{p-1} S\left(\frac{t(q-1)}{m}\right)$.

Proof. Notice that $\Phi(P) = \cdots P_t^{\text{ord}_{P_t}(\Phi(P))} \cdots$ and thus

$$\sigma_t \Phi(P) = \cdots P^{\text{ord}_{P_t}(\Phi(P))} \cdots$$

This gives

$$\text{ord}_P(\sigma_t \Phi(P)) = \text{ord}_{P_t}(\Phi(P)).$$

Choose t' so that $t' \equiv t \pmod{m}$ and $t' \equiv 1 \pmod{p}$. So $\sigma_{t'} : \zeta_p \mapsto \zeta_p^{t'} = \zeta_p$ and $\sigma_{t'} : \zeta_m \mapsto \zeta_m^{t'} = \zeta_m^t$. Then we have

$$\begin{aligned} \sigma_{t'}(g(P)) &= \sigma_{t'} \left(\sum_{\alpha \in F_q} \chi_P(\alpha) \psi(\alpha) \right) = \sum_{\alpha \in F_q} \sigma_{t'}(\chi_P(\alpha)) \sigma_{t'}(\psi(\alpha)) = \\ &= \sum_{\alpha \in F_q} \chi_P(\alpha)^{t'} \psi(\alpha)^{t'} = \sum_{\alpha \in F_q} \chi_P(\alpha)^t \psi(\alpha). \end{aligned}$$

Since $t \equiv t' \pmod{m}$ multiplication by t' will permute the elements of $\mathcal{Z}/m\mathcal{Z}$ the same as does multiplication by t . Thus $\sigma_{t'} \zeta_m^i = \zeta_m^{it'} = \zeta_m^{it} = \sigma_t \zeta_m^i$. So we have

$$\sigma_t(\Phi(P)) = \left(\sum_{\alpha \in F_q} \chi_P(\alpha)^t \psi(\alpha) \right)^m.$$

Applying Lemma 4.6.2 we get

$$\begin{aligned} g_{t\left(\frac{q-1}{m}\right)} &= \sum_{\alpha \in F_q} w^{-t\left(\frac{q-1}{m}\right)}(\alpha) \psi(\alpha) = \sum_{\alpha \in F_q} \left(w^{-\left(\frac{q-1}{m}\right)} \right)^t (\alpha) \psi(\alpha) = \\ &= \sum_{\alpha \in F_q} \chi_P(\alpha)^t \psi(\alpha), \end{aligned}$$

and thus

$$\sigma_t(\Phi(P)) = \left(g_{t\left(\frac{q-1}{m}\right)} \right)^m.$$

So we now have

$$\text{ord}_{\mathcal{P}}(\sigma_t(\Phi(P))) = (p-1) \text{ord}_{\mathcal{P}}(\sigma_t(\Phi(P))) = (p-1) \text{ord}_{P_t}(\Phi(P)).$$

Now applying Theorem 4.7.2 we have

$$\text{ord}_{\mathcal{P}}(\sigma_t(\Phi(P))) = \text{ord}_{\mathcal{P}} \left(g_{t\left(\frac{q-1}{m}\right)} \right)^m = m \cdot \text{ord}_{\mathcal{P}} \left(g_{t\left(\frac{q-1}{m}\right)} \right) = m \cdot S \left(t \frac{q-1}{m} \right).$$

Combining these we get

$$(p-1) \text{ord}_{P_t}(\Phi(P)) = m \cdot S \left(t \frac{q-1}{m} \right),$$

and therefore $\text{ord}_{P_t}(\Phi(P)) = \frac{m}{p-1} S \left(\frac{t(q-1)}{m} \right)$. \square

Finally we are ready to prove the Theorem of Stickelberger.

Theorem 4.7.5. (*Stickelberger*) $(\Phi(P)) = P^\gamma$ where

$$\gamma = \sum t\sigma_t^{-1}, \quad \text{where the sum is over all } t \text{ with } 1 \leq t < m, (t, m) = 1.$$

Proof. Note that

$$|\Phi(P)|^2 = \Phi(P)\overline{\Phi(P)} = g(P)^m \overline{g(P)^m} = (|g(P)|^2)^m = q^m = p^{fm},$$

so the only prime ideals in D_m containing $\Phi(P)$ are those containing p . So we have

$$\Phi(P) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}.$$

Pick \bar{p} with $1 \leq \bar{p} \leq m$ such that $p \equiv \bar{p} \pmod{m}$. We now examine the subgroup $\langle \bar{p} \rangle$ of $\mathcal{Z}/m\mathcal{Z}$. Since f is the smallest positive integer such that $p^f \equiv 1 \pmod{m}$ we know that $|\langle \bar{p} \rangle| = p^f$. Now consider $U(\mathcal{Z}/m\mathcal{Z})/\langle \bar{p} \rangle$. First note that the order of this quotient group is $\frac{\phi(m)}{f} = g$, which implies that there are g distinct left cosets of $\langle \bar{p} \rangle$. So we can pick $t_1, t_2, \dots, t_g \in U(\mathcal{Z}/m\mathcal{Z})$ such that the left cosets are $t_i \langle \bar{p} \rangle$, $1 \leq i \leq g$. So every element $t \in U(\mathcal{Z}/m\mathcal{Z})$ lies in exactly one of these cosets. Then for $t \in t_i \langle \bar{p} \rangle$ we can write $t = t_i p^j$ with $0 \leq j < f$. So for every $t \in U(\mathcal{Z}/m\mathcal{Z})$ there is a unique pair (i, j) , $1 \leq i \leq g$, $0 \leq j < f$ such that

$$t \equiv t_i p^j \pmod{m}.$$

Notice that there are $fg = \phi(m)$ possible pairs (i, j) . Using these t_i values we get via Lemma 4.7.4

$$\text{ord}_{P_i} \Phi(P) = \frac{m}{p-1} S \left(\frac{t_i(q-1)}{m} \right).$$

So we can now write

$$\begin{aligned} \Phi(P) &= P_1^{e_1} \cdots P_g^{e_g} = (\sigma_{t_1}^{-1} P)^{e_1} \cdots (\sigma_{t_g}^{-1} P)^{e_g} = \\ &= \prod_{i=1}^g (\sigma_{t_i}^{-1} P)^{\frac{m}{p-1} S \left(\frac{t_i(q-1)}{m} \right)}. \end{aligned}$$

We now simplify the exponent a bit. By Lemma 1.5.1 we have

$$\frac{m}{p-1} S \left(\frac{t_i(q-1)}{m} \right) = \frac{m}{p-1} (p-1) \sum_{j=0}^{f-1} \left\langle \frac{p^j t_i(q-1)}{q-1} \right\rangle = m \sum_{j=0}^{f-1} \left\langle \frac{p^j t_i}{m} \right\rangle,$$

so we have

$$\Phi(P) = \prod_{i=1}^g (\sigma_{t_i}^{-1} P)^{m \sum_{j=0}^{f-1} \langle \frac{p^j t_i}{m} \rangle}.$$

What we do now is just to make this last result look a bit neater. Write α^{σ_t} in place of $\sigma_t(\alpha)$ to obtain

$$\Phi(P) = P^{\sum_{i=1}^g m \sum_{j=0}^{f-1} \langle \frac{t_i p^j}{m} \rangle \sigma_{t_i}^{-1}} = P^{\gamma'},$$

where

$$\gamma' = m \sum_{i=1}^g \left(\sum_{j=0}^{f-1} \langle \frac{p^j t_i}{m} \rangle \right) \sigma_{t_i}^{-1}.$$

Since σ_p leaves P fixed, γ' has the same effect on P as

$$\begin{aligned} \gamma &= m \sum_i \sum_j \langle \frac{p^j t_i}{m} \rangle \sigma_{t_i}^{-1} \sigma_{p^j}^{-1} = \\ &= m \sum_{(t,m)=1; 1 \leq t \leq m} \langle \frac{t}{m} \rangle \sigma_t^{-1}. \end{aligned}$$

If $p^j t_i \equiv t \pmod{m}$, say $p^j t_i = t_0 m + t$, $0 \leq t < m$, then $\langle \frac{p^j t_i}{m} \rangle = \langle \frac{t}{m} \rangle = \frac{t}{m}$. So finally we have

$$\Phi(P) = P^{m \sum \frac{t}{m} \sigma_t^{-1}} = P^{\sum t \sigma_t^{-1}} = \prod_{1 \leq t \leq m; (t,m)=1} P^t.$$

□

Chapter 5

Some Difference Sets and Their p -Ranks

5.1 The Singer Difference Sets

Theorem 5.1.1. (*Singer Difference sets – Singer 1938*) For any prime power q and positive integer n , there is a (v, k, λ) -difference set D with

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^n - 1}{q - 1}, \quad \lambda = \frac{q^{n-1} - 1}{q - 1},$$

so that the resulting symmetric design is isomorphic to the design given by the points and hyperplanes of $PG(n, q)$.

Proof. First observe that the points and hyperplanes form a symmetric (v, k, λ) -design with parameters as given above. Then in view of Theorem 1.3.4 we need only show that there exists an automorphism of $PG(n, q)$ that permutes the points in a single cycle of length v , or equivalently so that the powers of the automorphism act transitively on the projective points. The points of $PG(n, q)$ are the 1-dimensional subspaces of an $(n + 1)$ -dimensional vector space V over F_q . Any nonsingular linear transformation T from V to itself will take subspaces to subspaces of the same dimension and thus gives an automorphism of $PG(n, q)$.

As an $(n + 1)$ -dimensional vector space over F_q , we choose $V := F_{q^{n+1}}$ as a vector space over its subfield F_q . Let w be a primitive element of $F_{q^{n+1}}$ and consider the linear transformation $T : x \mapsto wx$ of V over F_q . It is clear

that T is nonsingular and that its powers are transitive on the projective points. \square

This example also has an elegant description as a quotient set formulated in terms of the trace function $Tr : F_{q^{n+1}} \rightarrow F_q$.

Theorem 5.1.2. *Let q be a prime power and let $n \geq 2$ be an integer. Then*

$$D := \{xF_q^* : x \in F_{q^{n+1}}^* \text{ with } Tr(x) = 0\}$$

is a quotient set in $G := F_{q^{n+1}}^/F_q^*$ with parameters (v, k, λ) as in Theorem 5.1.1.*

Proof. For $x, y \in F_{q^{n+1}}^*$ with $xF_q^* = yF_q^*$, $Tr(x) = 0$ iff $Tr(y) = 0$. Since $Tr : F_{q^{n+1}}^* \rightarrow F_q$ is surjective, we have $|ker Tr| = q^n$. Thus $|D| = (q^n - 1)/(q - 1)$ as needed. Let $y \in F_{q^{n+1}}^* \setminus F_q^*$, so yF_q^* is a non-identity element of the quotient group G . We need to show that there are λ pairs of elements of D , say aF_q^* and bF_q^* for which $ab^{-1}F_q^* = yF_q^*$, i.e., $aF_q^* = ybF_q^*$. Since each element of the quotient group has $q - 1$ representatives, this means that we need to show that there are exactly $\lambda(q - 1)^2 = (q^{n-1} - 1)(q - 1)$ pairs (a, b) with $a, b \in F_{q^{n+1}}^*$, $Tr(yb) = Tr(b) = 0$, and $aF_q^* = ybF_q^*$. Since $\{x \in F_{q^{n+1}}^* : Tr(x) = 0\}$ and $\{x \in F_{q^{n+1}}^* : Tr(yx) = 0\}$ are different hyperplanes of the F_q -vector space $F_{q^{n+1}}$ with intersection of cardinality q^{n-1} , there are exactly $q^{n-1} - 1$ solutions $b \in F_{q^{n+1}}^*$ with $Tr(b) = Tr(yb) = 0$. For any such b , there are exactly $q - 1$ solutions of $a \in F_{q^{n+1}}^*$ with $aF_q^* = ybF_q^*$. Thus the number of pairs (a, b) satisfying the required conditions is exactly $(q^{n-1} - 1)(q - 1)$. \square

We now give a slightly different way to look at the second construction of the Singer difference sets and a genuinely different proof that they really exist. Here Tr represents the same trace function $Tr : F_{q^{n+1}} \rightarrow F_q$ as above. Recall that if $x \in F_{q^{n+1}}^*$ and $y \in F_q$, then $Tr(xy) = yTr(x)$. So for each coset xF_q^* of F_q^* in $F_{q^{n+1}}^*$, either $Tr(y) = 0$ for all $y \in xF_q^*$ or we may choose a coset representative x of xF_q^* such that $Tr(x) = 1$. So let L be a system of coset representatives of F_q^* in $F_{q^{n+1}}^*$ such that $Tr : L \rightarrow \{0, 1\}$. Write $L = L_0 \cup L_1$, where

$$L_0 = \{x \in L : Tr(x) = 0\}, \quad L_1 = \{x \in L : Tr(x) = 1\}.$$

Theorem 5.1.3. *With the above notation, L_0 is a $\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$ difference set in the quotient group $F_{q^{n+1}}^*/F_q^*$.*

Proof. Just for this proof put $F = F_{q^{n+1}}$. Let χ be a nontrivial multiplicative character of F^* whose restriction to F_q^* is trivial, so that we may view χ as a character of the quotient group F^*/F_q^* . It is easy to see that every nontrivial character of F^*/F_q^* can be obtained in this manner. First note that since $0 = \sum_{x \in F^*} \chi(x) = \sum_{a \in F_q^*} \sum_{x \in L} \chi(ax) = \sum_{x \in L} \chi(x) \sum_{a \in F_q^*} \chi_0(a) = \sum_{x \in L} \chi(x)(q-1)$ it must be that $\chi(L) = 0$ and $\chi(L_1) = -\chi(L_0)$.

Now let tr denote the trace function $tr : F \rightarrow F_p$. So for $x \in L$ and $a \in F_q^*$ we have $tr(ax) = tr_{q/p}(Tr(ax)) = tr_{q/p}(aTr(x))$. Also note that $\sum_{a \in F_q^*} \zeta_p^{Tr_{q/p}(a)} = \frac{q}{p} \sum_{i=0}^{p-1} \zeta_p^i = 0$, from which it follows that $\sum_{a \in F_q^*} \zeta_p^{Tr_{q/p}(a)} = 0 - \zeta_p^0 = -1$.

This gives

$$\begin{aligned}
g(\chi) &= \sum_{y \in F^*} \chi(y) \zeta_p^{tr(y)} = \sum_{a \in F_q^*} \sum_{x \in L} \chi(xa) \zeta_p^{tr(xa)} \\
&= \sum_{x \in L} \chi(x) \sum_{a \in F_q^*} \chi(a) \zeta_p^{tr_{q/p}(aTr(x))} \\
&= \sum_{x \in L_0} \chi(x) \sum_{a \in F_q^*} \chi_0(a) \zeta_p^{Tr_{q/p}(0)} + \sum_{x \in L_1} \chi(x) \sum_{a \in F_q^*} \chi_0(a) \zeta_p^{Tr_{q/p}(a)} \\
&= (q-1)\chi(L_0) + \chi(L_1) \sum_{a \in F_q^*} \zeta_p^{Tr_{q/p}(a)} \\
&= (q-1)\chi(L_0) - \chi(L_0)(-1) = q\chi(L_0). \tag{5.1}
\end{aligned}$$

By Theorem 4.4.2 we have $g(\chi)\overline{g(\chi)} = q^{n+1}$, so that by Eq. 5.1 we have $\chi(L_0)\overline{\chi(L_0)} = q^{n-1} = \frac{q^n-1}{q-1} - \frac{q^{n-1}-1}{q-1} = k - \lambda$. The proof is now completed by applying Theorem 1.4.4. \square

Theorem 5.1.4. For $q = p^f$, let L_0 be the $\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$ difference set in the quotient group $F_{q^{n+1}}^*/F_q^*$ as in Theorem 5.1.3. Then the p -rank of L_0 is

$$\binom{p+n-1}{n}^f + 1.$$

Proof. Let \mathcal{P} be a prime ideal in $D_{q^{n+1}-1}$ lying over p . So $\bar{1}, \bar{\zeta}_{q^{n+1}-1}, \dots, \bar{\zeta}_{q^{n+1}-1}^{q^{n+1}-2}$ are the distinct nonzero residues modulo \mathcal{P} . Let $w_{\mathcal{P}}$ be the Teichmüller character on $F = F_{q^{n+1}}$. In particular, $w_{\mathcal{P}}(\bar{\zeta}_{q^{n+1}-1}^i) = \zeta_{q^{n+1}-1}^i$.

As $w_{\mathcal{P}}$ has order $q^{n+1} - 1$ and generates the group of characters on F^* , the character $\chi = w_{\mathcal{P}}^{-(q-1)}$ has order $\frac{q^{n+1}-1}{q-1}$ and is a generator of the character group of F^*/F_q^* . From the proof of Theorem 5.1.3 (see Eq. 5.1) we know that for each a , $0 < a < \frac{q^{n+1}-1}{q-1}$,

$$q \cdot \chi^a(L_0) = g(\chi^a). \quad (5.2)$$

By Corollary 1.4.7 we know the p -rank of L_0 is the number of characters χ of F^*/F_q such that $\chi(L) \not\equiv 0 \pmod{\mathcal{P}}$. For the trivial character χ_0 we have $\chi_0(L_0) = |L_0| = \frac{q^{n+1}-1}{q-1} \not\equiv 0 \pmod{\mathcal{P}}$. So the p -rank of L_0 is $1 + A(q, n+1)$, where $A(q, n+1)$ is the number of χ^a with $0 < a < \frac{q^{n+1}-1}{q-1}$ such that $\chi^a(L_0) \not\equiv 0 \pmod{\mathcal{P}}$.

Let \mathcal{B} be the (unique) prime of $D_{p(q^{n+1}-1)}$ lying over \mathcal{P} . Since \mathcal{B} divides $\chi^a(L_0)$ if and only if \mathcal{P} divides $\chi^a(L_0)$, $A(q, n+1)$ is equal to the number of χ^a , $0 < a < \frac{q^{n+1}-1}{q-1}$, such that $\chi^a(L_0) \not\equiv 0 \pmod{\mathcal{B}}$.

By the definition of $\tilde{s}(a)$ (with q^{n+1} in place of q), $\mathcal{B}^{\tilde{s}((q-1)a)} \parallel g(\chi^a)$. Since $\mathcal{B}^{(p-1)f} \parallel q$, we see from Eq. 5.2 that $A(q, n+1)$ is equal to the number of a , $0 < a < \frac{q^{n+1}-1}{q-1}$, such that $\tilde{s}((q-1)a) = (p-1)f$, which, in turn, is equal to the number of x , $0 < x < q^{n+1} - 1$, with $(q-1)|x$, such that $\tilde{s}(x) = (p-1)f$.

For x with $0 < x < q^{n+1} - 1$, first write x to the base q : $x = \sum_{j=0}^n b_j q^j$, with $0 \leq b_j \leq q-1$. Then write each b_j to the base p as $b_j = \sum_{i=0}^{f-1} x_{i,j} p^i$, $0 \leq x_{i,j} < p$. So

$$x = \sum_{j=0}^n \sum_{i=0}^{f-1} x_{i,j} p^i q^j, \quad 0 \leq x_{i,j} < p.$$

By Theorem 4.7.2 and Eq. 1.21 (with q^{n+1} in place of q),

$$\tilde{s}(x) = \frac{p-1}{q^{n+1}-1} \sum_{j=0}^n \sum_{i=0}^{f-1} L(x p^i q^j), \quad (5.3)$$

where $L(y)$ denotes the reduction of y modulo $q^{n+1}-1$. Suppose that $(q-1)|x$ and $\tilde{s}(x) = (p-1)f$. Then, by Eq. 5.3

$$(q^{n+1}-1)f = \sum_{j=0}^n \sum_{i=0}^{f-1} L(x p^i q^j). \quad (5.4)$$

If we put $x = (q - 1)y$, then for fixed i ,

$$0 < \sum_{j=0}^n L(xp^i q^j) \equiv \sum_{j=0}^n xp^i q^j = p^i y (q-1)(1+q+\cdots+q^{f-1}) \equiv 0 \pmod{q^{n+1}-1},$$

it follows that $\sum_{j=0}^n L(xp^i q^j) \geq q^{n+1} - 1$ for each i . Thus by Eq. 5.4 we must have

$$\sum_{j=0}^n L(xp^i q^j) = q^{n+1} - 1 \quad (5.5)$$

for each i .

Since $x = b_0 + b_1 q + \cdots + b_n q^n$ with $i = 0$ in Eq. 5.5, we have

$$\begin{aligned} q^{n+1} - 1 &= \sum_{j=0}^n L((b_0 + b_1 q + \cdots + b_n q^n) q^j) = \\ &= \sum_{j=0}^n \left(\sum_{k=0}^n b_{[k-j]} q^k \right) = \text{(where a subscript } [r] \text{ is to be reduced modulo } n+1) \\ &= \sum_{k=0}^n \left(\sum_{j=0}^n b_{[k-j]} \right) q^k = \left(\sum_{j=0}^n b_j \right) \sum_{k=0}^n q^k = \\ &= \left(\sum_{j=0}^n b_j \right) \cdot \frac{q^{n+1} - 1}{q - 1}, \text{ which implies } \sum_{j=0}^n b_j = q - 1. \end{aligned}$$

Hence

$$\begin{aligned} q - 1 &= \sum_{j=0}^n \sum_{i=0}^{f-1} x_{i,j} p^i = \sum_{i=0}^{f-1} \left(\sum_{j=0}^n x_{i,j} \right) p^i = \\ &= \sum_{j=0}^n x_{0,j} + p \sum_{i=1}^{f-1} \left(\sum_{j=0}^n x_{i,j} \right) p^{i-1}. \end{aligned} \quad (5.6)$$

This implies

$$q - 1 \equiv p - 1 \equiv \sum_{j=0}^n x_{0,j} \pmod{p}.$$

Since $x_{0,j} \geq 0$ for all j , this implies $\sum_{j=0}^n x_{0,j} \geq p - 1$.

Our next step is to show that for each r with $1 \leq r \leq f - 1$ we also have that

$$\sum_{j=0}^n x_{r,j} \geq p - 1.$$

So fix r in this range. Suppose $xp^r \equiv \sum_{k=0}^n a_k q^k \pmod{q^{n+1} - 1}$. The symbol $a_{[t]}$ means that the subscript t is to be reduced modulo $n + 1$ to lie in the range $0 \leq t \leq n$. By Eq. 5.5 we have

$$\begin{aligned} q^{n+1} - 1 &= \sum_{j=0}^n L(xp^r q^j) = \sum_{j=0}^n L\left(\sum_{k=0}^n a_k q^k\right) q^j = \\ &= \sum_{j=0}^n L\left(\sum_{k=0}^n a_{[k-j]} q^k\right) = \sum_{k=0}^n \left(\sum_{j=0}^n a_{[k-j]}\right) q^k = \\ &= \sum_{j=0}^n a_{[j]} \cdot \sum_{k=0}^n q^k = \sum_{j=0}^n a_j \cdot \frac{q^{n+1} - 1}{q - 1}. \end{aligned}$$

This forces

$$q - 1 = \sum_{j=0}^n a_j. \tag{5.7}$$

We now take a hard look at the a_j .

$$\begin{aligned} xp^r &= \sum_{j=0}^n b_j q^j p^r = \sum_{j=0}^n \left(\sum_{i=0}^{f-1} x_{i,j} p^i\right) p^{r+fj} = \\ &= \sum_{i=0}^{f-1} \sum_{j=0}^n x_{i,j} p^{fj+i+r} = \sum_{t=0}^n a_t q^t, \end{aligned}$$

where

$$a_t q^t = \sum_{i=f-r}^{f-1} x_{i,t-1} p^{(t-1)f+i+r} + \sum_{i=0}^{f-1-r} x_{i,t} p^{tf+i+r},$$

from which we conclude

$$a_t = x_{[f-r,t-1]} + x_{[f-r+1,t-1]}p + \cdots + x_{[f-1,t-1]}p^{r-1} + x_{0,t}p^r + \cdots + x_{[f-1-r,t]}p^{f-1}.$$

Here $x_{[i,j]}$ means that the index i is reduced modulo f and the index j is reduced modulo $n+1$. Now consider Eq. 5.7 modulo p .

$$q - 1 \equiv p - 1 \equiv \sum_{j=0}^n x_{f-r,j} \pmod{p}.$$

Since $x_{i,j} \geq 0$ in all cases, we must have

$$\sum_{j=0}^n x_{i,j} \geq p - 1 \text{ for all } i. \quad (5.8)$$

Recall that we are looking for all the x , $0 < x < q^{n+1} - 1$ with $\tilde{s}(x) = (p-1)f$. We now have

$$(p-1)f \leq \sum_{i=0}^{f-1} \sum_{j=0}^n x_{i,j} = S(x) = \tilde{s}(x) = (p-1)f,$$

from which we have that equality holds in Eq. 5.8 for each i . The equation $\sum_{j=0}^n x_{i,j} = p - 1$, $0 \leq x_{i,j} < p$, has $\binom{p+n-1}{n}$ solutions for each i , $0 \leq i < f$. (See Eq. 1.10 of 6409 notes.) Therefore $A(q, n+1) = \binom{p+n-1}{n}^f$. This completes the proof. \square

5.2 Monomial Hyperovals and Difference Sets

Warning to the reader: Unfortunately, after this section was written it was noticed that the symbol k is being used in two ways. It is the k of the (v, k, λ) -design, and it is the k of the hyperoval $D(x^k)$. Given this advanced warning, the reader should be able to keep straight the two uses of k in the same sentence.

Let $D(x^k)$ be a monomial hyperoval in $PG(2, q)$, $q = 2^f$. So $(k, q-1) = (k-1, q-1) = 1$. Put $D_{k,q} = \{x^k + x : x \in F_q \setminus F_2\}$.

Theorem 5.2.1. $D_{k,q}$ is a $(q-1, q/2-1, q/4-1)$ -quotient set in F_q^* .

Proof. Let χ be any nontrivial multiplicative character of F_q^* , so also $\chi(0) = 0$. Since $(k-1, q-1) = 1$ there must be a multiplicative character ϕ of F_q^* for which $\chi = \phi^{k-1}$. Recall that $x \mapsto x^k + x$ is a two-to-one mapping. Hence

$$\begin{aligned} \chi(D_{k,q}) &= \frac{1}{2} \sum_{x \in F_q} \chi(x^k + x) = \frac{1}{2} \sum_{x \in F_q} \chi(x) \chi(1 + x^{k-1}) = \\ &= \frac{1}{2} \sum_{x \in F_q} \phi(x^{k-1}) \chi(1 + x^{k-1}) = \frac{1}{2} J(\phi, \chi) = \frac{1}{2} J(\phi, \phi^{k-1}). \end{aligned} \quad (5.9)$$

Note that ϕ , ϕ^{k-1} and ϕ^k are all nontrivial. By Theorem 4.4.4 $\chi(D_{k,q}) \overline{\chi(D_{k,q})} = \frac{1}{4} J(\phi, \phi^{k-1}) \overline{J(\phi, \phi^{k-1})} = q/4$. So $v = |F_q^*| = q-1$, $k = |D_{k,q}| = q/2 - 1$, and $k - \lambda = q/4$, so that $\lambda = q/4 - 1$. \square

We recall the following (see FGQ, Theorem 12.5.3):

Theorem 5.2.2. *Let $q > 2$ be a power of 2. Two monomial hyperovals $D(x^j)$ and $D(x^k)$ in $PG(2, q)$ are projectively equivalent if and only if $j \equiv k, 1/k, 1-k, 1/(1-k), k/(k-1),$ or $k-1/k \pmod{q-1}$.*

The following theorem shows that two projectively equivalent monomial hyperovals give rise to two equivalent cyclic difference sets under the construction of Theorem 5.2.1.

Theorem 5.2.3. *Let $q = 2^f$, $q > 2$. If $D(x^k)$ and $D(x^j)$ are two projectively equivalent monomial hyperovals in $PG(2, q)$, the the corresponding difference sets $D_{k,q}$ and $D_{j,q}$ constructed in Theorem 5.2.1 are equivalent.*

Proof. Recall the definition of equivalence of quotient sets from Section 1.3. ($D_1^\alpha = aD_2$) Then the proof follows from Theorem 5.2.2 and the following:

$$D_{\frac{k}{k-1}, q} = D_{\frac{k-1}{k}, q} = D_{k,q}^{(k-1)}, \quad (5.10)$$

$$D_{1-k, q} = D_{\frac{1}{1-k}, q} = D_{k,q}^{\left(\frac{1-k}{k}\right)}, \quad (5.11)$$

$$D_{\frac{1}{k}, q} = D_{k,q}. \quad (5.12)$$

\square

The difference sets $D_{2^i, q}$, $(i, f) = 1$, arising from the regular and translation hyperovals are the Singer difference sets $\{y \in F_q^* : \text{Tr}(y) = 0\}$. This follows from Theorem 1.2.1, Theorem 5.1.2, and the definition of $D_{k, d}$. It is our intention to study the 2-ranks of these cyclic difference sets arising from the monomial hyperovals to show that the translation hyperovals, the Segre hyperovals, and the two families of Glynn hyperovals all give inequivalent cyclic difference sets.

Theorem 5.2.4. *Let $D_{k, q}$ be the $(q - 1, q/2 - 1, q/4 - 1)$ cyclic difference set in F_q^* constructed from the hyperoval $D(x^k)$ as in Theorem 5.2.1. Then let $\overline{D_{k, q}}$ be the complement of $D_{k, q}$ in F_q^* , so $\overline{D_{k, q}}$ is a $(q - 1, q/2, q/4)$ cyclic difference set in F_q^* . Then the 2-rank of $\overline{D_{k, q}}$ is equal to the number of a 's, $0 < a < 2^f - 1$, such that*

$$\tilde{s}(a) + \tilde{s}((k - 1)a) = \tilde{s}(ka) + 1,$$

where $\tilde{s}(a)$ is as defined as in Lemma 4.7.1 (see also Theorem 4.7.2) with $q = 2^f$.

Proof. Using the notation adopted in Section 4.5 we let \mathcal{B} be a prime ideal in D_{q-1} lying over 2, and let $w = w_{\mathcal{B}}$ be the Teichmüller character on F_q . If χ is a nontrivial multiplicative character on F_q^* , then $\chi(F_q^*) = 0$, so $\chi(\overline{D}) = -\chi(D)$.

By Eq. 5.9 (multiplied by $p = 2$) we see that for each a , $0 < a < q - 1$, with $\phi = w^{-a}$, $\chi = \phi^{k-1} = w^{-(k-1)a}$,

$$2w^{-(k-1)a}(\overline{D_{k, q}}) = -2w^{-(k-1)a}(D_{k, q}) = -J(w^{-a}, w^{-(k-1)a}),$$

so

$$-2 \cdot w^{-(k-1)a}(\overline{D_{k, q}}) = J(w^{-a}, w^{-(k-1)a}). \quad (5.13)$$

By Theorem 4.4.4 we have

$$J(w^{-a}, w^{-(k-1)a}) = \frac{g(w^{-a})g(w^{-(k-1)a})}{g(w^{-ka})}.$$

By definition of \tilde{s} we have that $\mathcal{B}^{\tilde{s}(a)} \parallel g(w^{-a})$. So putting these two facts together we have

$$\mathcal{B}^{\tilde{s}(a) + \tilde{s}((k-1)a) - \tilde{s}(ka)} \parallel J(w^{-a}, w^{-(k-1)a}). \quad (5.14)$$

Since $\mathcal{B} \parallel 2$, by Eq. 5.13 $w^{-(k-1)a}(\overline{D_{k, q}})$ is not zero modulo \mathcal{B} if and only if $\mathcal{B} \parallel J(w^{-a}, w^{-(k-1)a})$, which by Eq. 5.14 is if and only if $\tilde{s}(a) + \tilde{s}((k - 1)a) -$

$\tilde{s}(ka) = 1$. Since w generates the character group of F_q^* , the number of a , $0 < a < q-1$, with $w^{-(k-1)a}(\overline{D}_{k,q})$ not zero mod \mathcal{B} is the number of nontrivial characters χ on F_q^* with $\chi(\overline{D}_{k,q})$ not zero mod \mathcal{B} . Since the cardinality of $\overline{D}_{k,q}$ is $q/2 \equiv 0 \pmod{2}$, the trivial character is not counted here. Hence by Corollary 1.4.7 the 2-rank of $\overline{D}_{k,q}$ is the number of a 's, $0 < a < q-1$, for which $\tilde{s}(a) + \tilde{s}((k-1)a) = \tilde{s}(ka) + 1$. \square

5.3 p -Ranks of The Segre Hyperovals $D(x^6)$

In this section we put $k = 6$ and $q = 2^f$ with f odd to obtain the Segre hyperoval. For completeness (and because it is rather simple) we show that this really does give a hyperoval. By Theorem 1.6.1 it suffices to show that for $0 \neq s \in F_q$ the map $x \mapsto f_s(x) = \begin{cases} \frac{f(x+s)+f(s)}{x}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0, \end{cases}$ is a permutation.

Put $x = ts$ to see that $f_s(x) = s^5(t^5+t^3+t)$, so for $s \neq 0$ it suffices to show that $t \mapsto t^5+t^3+t$ is a permutation. So suppose that $t^5+t^3+t = u^5+u^3+u$. This implies that

$$\begin{aligned} 0 &= (t+u)[t^4+t^3u+t^2u^2+tu^3+u^4+t^2+tu+u^2+1] = \\ &= (t+u)[(t^2+u^2+1)^2+(t^2+u^2+1)(tu+1)+(tu+1)^2]. \end{aligned}$$

Since f is odd, $z^2+zw+w^2 = 0$ has no solution in F_q , implying that $x \mapsto f_s(x)$ is a permutation. Hence the Segre hyperoval really is a hyperoval. '

In fact we have already done all the work to determine the 2-rank of the difference set arising from the Segre hyperoval.

Theorem 5.3.1. *Let $f = 2n + 1$ be an odd integer, $f \geq 5$, $q = 2^f$, $F = F_q$, and let $D_{6,q}$ be the $(q-1, q/2-1, q/4-1)$ cyclic difference set in F^* corresponding to the Segre hyperoval $D(x^6)$. Let $\overline{D}_{6,q}$ be the complement of $D_{6,q}$ in F^* . Then the 2-rank $B_6(f)$ of $\overline{D}_{6,q}$ is equal to $f(2F_{(f-1)/2} - 1)$, where F_n is the n th Fibonacci number ($F_0 = F_1 = 1$).*

Proof. Since $\tilde{s}(a) = S(a)$, if $k = 6$, then by Theorem 1.5.9 the number of solutions to Eq. 1.26, i.e., to the equality of Theorem 5.2.4 is $B_6(2n+1) = (2n+1)(2F_n - 1)$, where F_n is the n th Fibonacci number. \square

Note: From the well known formula for the Fibonacci numbers we see that

$$B_6(2n+1) = (2n+1) \left\{ \frac{2}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \frac{2}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} - 1 \right\}.$$

We now consider the equation $x^6 + x + b = 0$ in $F = F_q$. Choose a fixed generator α of F^* , $q = 2^f$. Keep in mind that $D_{6,q} = \{x^6 + x : x \in F \setminus F_2\}$. Define the polynomial $\theta(x)$ over F_2 by

$$\theta(x) = \sum_{j=0}^{q-2} b_j x^j, \text{ where } b_j = \begin{cases} 1, & \text{if } \alpha^j \in D_{6,q}, \\ 0, & \text{if } \alpha^j \notin D_{6,q}. \end{cases} \quad (5.15)$$

For $\sigma \in \text{Aut}(F)$, $\alpha^j \in D_{6,q}$ iff $(\alpha^j)^\sigma \in D_{6,q}$. It follows easily that $\theta(\alpha^i)$ is also fixed under σ , so we have

$$\theta(\alpha^i) \in F_2. \quad (5.16)$$

Now let \mathcal{B} be a prime ideal of D_{q-1} lying over 2. Let $w = w_{\mathcal{B}}$ be the Teichmüller character on F . So $w(\alpha^j) \pmod{\mathcal{B}}$ is actually equal to α^j , from which we see

$$\text{The equivalence class modulo } \mathcal{B} \text{ of } w^i(\alpha^j) \text{ is actually equal to } \alpha^{ij}. \quad (5.17)$$

Now consider

$$\begin{aligned} w^i(D_{6,q}) &= \sum_{\alpha^j \in D_{6,q}} w^i(\alpha^j), \text{ which modulo } \mathcal{B} \text{ is equal to} \\ &\sum_{\alpha^j \in D_{6,q}} \alpha^{ij} = \sum_{j=0}^{q-2} b_j \alpha^{ij} = \theta(\alpha^i). \end{aligned}$$

This implies

$$w^{-5a}(D_{6,q}) \pmod{\mathcal{B}} \text{ is equal to } \theta(\alpha^{-5a}). \quad (5.18)$$

Use Eq. 5.9 with $\chi = w^{-5a}$, viz.,

$$2 \cdot w^{-5a}(D_{6,q}) = J(w^{-a}, w^{-5a}) = \frac{g(w^{-a})g(w^{-5a})}{g(w^{-6a})}.$$

Since $\mathcal{B} \parallel 2$ and since $S(a) = \tilde{s}(a)$, implying $\mathcal{B}^{S(a)+S(5a)-S(6a)} \parallel 2 \cdot w^{-5a}(D_{6,q})$, we see that \mathcal{B} does not divide $w^{-5a}(D_{6,q})$ iff $S(a) + S(5a) - S(6a) = 1$. Also, $\theta(1) = |D_{6,q}| = q/2 - 1 \equiv 1 \pmod{2}$, so $\theta(1) = 1 \neq 0$. So by Eq. 5.18 we have

$$\theta(\alpha^{-i}) = \begin{cases} 1, & \text{if } i = 0 \text{ or } i = 5a \text{ and } S(a) + S(5a) = S(6a) + 1; \\ 0, & \text{otherwise.} \end{cases} \quad (5.19)$$

From the proof of Lemma 1.5.7 we know that if $\mathcal{S} = \{a : 0 < a < q - 1 \text{ and } S(a) + S(5a) = S(6a) + 1\}$, then for $a \in \mathcal{S}$, $a, a \cdot 2, a \cdot 2^2, a \cdot 2^3, \dots, a \cdot 2^{f-1}$ all belong to \mathcal{S} and are distinct modulo $q - 1$. This is a *cyclotomic coset* of size f . Let J be a set of distinct cyclotomic coset representatives of the elements of \mathcal{S} . Then

$$(\alpha^j)^{5a} + (\alpha^j)^{5a \cdot 2} + (\alpha^j)^{5a \cdot 2^2} + \dots + (\alpha^j)^{5a \cdot 2^{f-1}} = \text{Tr}(\alpha^{j5a}).$$

By Theorem 1.2.4 (iii),

$$\begin{aligned} b_j &= - \sum_{i=0}^{q-2} \theta(\alpha^{-i})(\alpha^i)^j = 1 + \sum_{a \in \mathcal{S}} (\alpha^j)^{5a} = \\ &= 1 + \sum_{a \in J} \text{Tr}((\alpha^j)^{5a}) = 1 \text{ iff } \sum_{a \in J} \text{Tr}((\alpha^j)^{5a}) = 0. \end{aligned}$$

This says $b = \alpha^j \in D_{6,q}$ iff $\sum_{a \in J} \text{Tr}((\alpha^j)^{5a}) = 0$, which proves the following theorem. (Put $b = \alpha^j$.)

Theorem 5.3.2. *Let $q = 2^f$ with f odd. Then for $b \in F = F_q$, $x^6 + x + b = 0$ has a solution (and hence exactly two solutions) in F if and only if $\sum_{a \in J} \text{Tr}(b^{5a}) = 0$.*

5.4 p -Ranks of the Glynn Hyperovals $D(x^{3\sigma+4})$.

In this section we again assume that $q = 2^f$ with f odd and put $k = 3\sigma + 4$, where $\sigma^2 = 2$. This gives a family of hyperovals $D(x^{3\sigma+4})$ due to D. Glynn. Unfortunately in this case it is rather difficult to show that $D(x^{3\sigma+4})$ really is a hyperoval. Our course notes [Pa05] have an interesting proof by W. E. Cherowitzo, and Glynn's original proof (see [Gl83]) is reproduced in [PT84].

This section was written by S. Flink.

This is merely a rehashing of pages 96-98 of the paper [EHKX99] with some details filled in; no claims of originality are made. Let $B_{3\sigma+4}(d)$ be the number of solutions a , $0 < a < 2^d - 1$ to the equation

$$s(a) + s((k - 1)a) = s(ka) + 1. \tag{5.20}$$

In the proof of Theorem 4.1 from the paper [EHKX99] it is shown that the solutions to Eq. 5.20 are completely characterized by the following property:

There is exactly one instance of a 1 occurring in the same place in a and in $(k - 1)a$, and immediately to the left of those 1's there is a 0 in both a and in $(k - 1)a$, (5.21)

(5.22)

where we view a and $(k - 1)a \pmod{2^d - 1}$ as binary strings of length d .

Our intent here is to fill in the details to Theorem 4.6 in the paper, which we restate here.

Theorem 5.4.1. *Let d be an odd integer, $d \geq 3$. Let $B_{3\sigma+4}(d)$ be defined as above and let $A_{3\sigma+4}(d) = B_{3\sigma+4}(d)/d$. Then*

$$\begin{aligned} A_{3\sigma+4}(d) = & A_{3\sigma+4}(d - 2) + 3A_{3\sigma+4}(d - 4) \\ & - A_{3\sigma+4}(d - 6) - A_{3\sigma+4}(d - 8) + 1 \end{aligned}$$

for all odd d , $d \geq 11$, with the following initial values:

| | | | | | | | | | | | | |
|--------------------|---|---|---|---|----|----|----|-----|-----|-----|------|------|
| d | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 |
| $A_{3\sigma+4}(d)$ | 1 | 1 | 5 | 7 | 21 | 37 | 89 | 173 | 383 | 777 | 1665 | 3441 |

Proof. Note that if a is a solution to 5.20 then any rotation of a is a solution as well, so we will restrict our attention at present to those solutions where the instance of a 1 imposed by 5.21 occurs in the middle of a string. We call such a solution a *special* solution.

To prove the theorem, we define a bijection between these special solutions to equation 5.20 and a set of closed walks in a certain directed graph D . Once this bijection is established, it follows from first principles (actually

an application of transfer-matrix theory) that the generating function for the number of these closed walks is rational. We then check 5.23 (on a computer) for enough odd values of d so that Lemma 4.5 in the paper will imply that 5.23 must hold for all odd $d \geq 11$.

Let $d = 2r - 1$ and look at the computation of $(k - 1)a$ and ka . Since $k - 1 = 3\sigma + 3 = 3 \cdot 2^{(d+1)/2} + 3 = 2^{r+1} + 2^r + 2^1$ we may compute $(k - 1)a$ and $ka \pmod{2^d - 1}$ as

$$\begin{array}{rcccccccc}
 a & = & a_{2r-2} & \cdots & a_r & a_{r-1} & a_{r-2} & \cdots & a_0 \\
 2a & = & a_{2r-3} & \cdots & a_{r-1} & a_{r-2} & a_{r-3} & \cdots & a_{2r-2} \\
 2^{r+1}a & = & a_{r-3} & \cdots & a_{2r-2} & a_{2r-3} & a_{2r-4} & \cdots & a_{r-2} \\
 + \quad 2^r a & = & a_{r-2} & \cdots & a_0 & a_{2r-2} & a_{2r-3} & \cdots & a_{r-1} \\
 \hline
 (k-1)a & = & y_{2r-2} & \cdots & y_r & y_{r-1} & y_{r-2} & \cdots & y_0 \\
 + \quad a & = & a_{2r-2} & \cdots & a_r & a_{r-1} & a_{r-2} & \cdots & a_0 \\
 \hline
 ka & = & z_{2r-2} & \cdots & z_r & z_{r-1} & z_{r-2} & \cdots & z_0
 \end{array} \tag{5.23}$$

where

$$a_i + a_{i-1} + a_{r+i-2} + a_{r+i-1} + b_{i-1} = y_i + 2b_i \text{ and} \tag{5.24}$$

$$y_i + a_i + c_{i-1} = z_i + 2c_i \text{ for } i = 0, 1, \dots, 2r - 2, \tag{5.25}$$

for some integers b_i, c_i with $0 \leq b_i \leq 3$ and $c_{r-1} = 1$ and $c_i = 0$ for $i = 0, 1, \dots, r - 2, r, \dots, 2r - 2$, where the indices are read modulo $2r - 1$ throughout.

The integer b_i is the carry-over from the i th place to the $(i + 1)$ st place during the addition that gives $(k - 1)a$ above. One may verify inductively by adding columns of four 1's that the b_i never exceed 3. The integer c_i is the carry over from the i th place to the $i + 1$ st place during the addition of $(k - 1)a$ and a and the above restriction reflects the restriction imposed by 5.21. The addition in equation 5.23 is carried out in base 2, but the following equations 5.24 and 5.25 for y_i and z_i only concern the individual columns. To see what 5.24 and 5.25 represent, carry out the addition in three steps. First add each column, including the number of 1's that would have been carried over from the previous column; this is $a_i + a_{i-1} + a_{r+i-2} + a_{r+i-1} + b_{i-1}$, which is equal to the digit in the (eventual) binary representation, plus 2 times the number of 1's carried into the next column. The next step is to convert to binary notation, proceeding from left to right. We now have an ordinary binary number, which we rewrite mod $2^d - 1$ by noting that a 1 in the $d + 1$ st place equals $1 \pmod{2^d - 1}$. When the addition is carried out as above, it is

clear that there is a unique choice of b_i 's and c_i 's which satisfy 5.24 and 5.25 such that the y_i 's and z_i 's are the digits given by 5.23, where addition has been carried out modulo $2r - 1$.

The following procedure is a way of counting all possible sets of d -tuples which can comprise the columns of the tableau 5.23 subject to the restrictions imposed by equations 5.24 and 5.25. In order to make this procedure clearer, we begin with a relabeling of the sequences in these equations. Given the sequence (x_i) , which can be any of (a_i) , (b_i) , (c_i) , (y_i) or (z_i) for $i = 0, \dots, 2r - r$, define (\tilde{x}_j) , $j = 0, \dots, 2r - 2$ by $\tilde{x}_j := x_{(r-1)i}$. Note that since $(r - 1, 2r - 1) = 1$, the sequence (\tilde{x}_j) is a permutation of (x_i) , since the indices are read modulo $2r - 1$. Put $i = (r - 1)j$ in 5.24 and 5.25 and use $-1 \equiv 2r - 2 \pmod{2r - 1}$ to obtain permuted subscripts:

$$\begin{array}{cccc} (r-1)j & (r-1)j-1 & r+(r-1)j-2 & r+(r-1)j-1 \\ \parallel & \parallel & \parallel & \parallel \\ (r-1)j & (r-1)j+2r-2 & (r-1)j+(r-1)-1 & (r-1)j+(r-1) \\ \downarrow & \downarrow & \downarrow & \downarrow \\ j & j+2 & j+3 & j+1 \end{array}$$

and equations 5.24 and 5.25 become

$$\tilde{a}_j + \tilde{a}_{j-1} + \tilde{a}_{r+j-2} + \tilde{a}_{r+j-1} + \tilde{b}_{j-1} = \tilde{y}_j + 2\tilde{b}_j \text{ and} \quad (5.26)$$

$$\tilde{y}_j + \tilde{a}_j + \tilde{c}_{j-1} = \tilde{z}_j + 2\tilde{c}_j \text{ for } j = 0, 1, \dots, 2r - 2, \quad (5.27)$$

where indices are taken mod $2r - 1$ and $0 \leq \tilde{b}_j \leq 3$ for all j and $\tilde{c}_1 = 1$ and $\tilde{c}_j = 0$ whenever $j \neq 1$.

We will now construct a directed graph D whose vertex set is the set of all vectors $(a', a'', a''', b', b'', c', c'')$ with $0 \leq a', a'', a''' \leq 1$, $0 \leq b', b'' \leq 3$ and $0 \leq c', c'' \leq 1$. If we fix a special solution a to

$$s(a) + s((k-1)a) = s(ka) + 1$$

with $k = 3\sigma + 4 = 3 \cdot 2^{\frac{d+1}{2}} + 4$ and define vertices

$$v_j = (\tilde{a}_j, \tilde{a}_{j+1}, \tilde{a}_{j+2}, \tilde{b}_j, \tilde{b}_{j+1}, \tilde{c}_j, \tilde{c}_{j+1})$$

for $j = 0, \dots, 2r - 2$. Then the orientation of D which we are about to define will put a in correspondence with the closed walk

$$v_0 \rightarrow v_1 \rightarrow \dots \rightarrow v_{2r-2} \rightarrow v_0$$

and further, each such closed walk will correspond to a unique solution a .

We connect a vertex $(a', a'', a''', b', b'', c', c'')$ to a vertex $(A', A''A'', B', B'', C', C'')$ by a directed edge if and only if

$$a'' = A' \quad (5.28)$$

$$a''' = A'' \quad (5.29)$$

$$b'' = B' \quad (5.30)$$

$$c'' = C' \quad (5.31)$$

subject to

$$Y := (a' + a''' + A''' + a'' + B'' - 2b') \in \{0, 1\} \quad (5.32)$$

$$Z := (Y + a' + C'' - 2c') \in \{0, 1\}. \quad (5.33)$$

To motivate the construction of the directed edges, the reader should think of

$$(a', a'', a''', b', b'', c', c'') \text{ and } (A', A''A'', B', B'', C', C'')$$

as

$$v_j = (\tilde{a}_j, \tilde{a}_{j+1}, \tilde{a}_{j+2}, \tilde{b}_j, \tilde{b}_{j+1}, \tilde{c}_j, \tilde{c}_{j+1}) \text{ and } v_{j+1} = (\tilde{a}_{j+1}, \tilde{a}_{j+2}, \tilde{a}_{j+3}, \tilde{b}_{j+1}, \tilde{b}_{j+2}, \tilde{c}_{j+1}, \tilde{c}_{j+2})$$

respectively, for $j = 0, 1, \dots, 2r - 2$. Observe that 5.32 reflects 5.26 and that 5.33 reflects 5.27.

Define V_0 , V_1 , and V_2 as the sets of vertices $(a', a'', a''', b', b'', c', c'')$ for which (c', c'') equals $(0, 0)$, $(0, 1)$, and $(1, 0)$, respectively. We note first that those vertices with $(c', c'') = (1, 1)$ can never yield a solution, as this case is equivalent to having a 1 in both the j th and $(j + 1)$ st position in both a and $(k - 1)a$, violating 5.21. With the preceding definitions, we claim that for odd $d \geq 3$, the special solutions a , $0 < a < 2^d - 1$, to equation 5.20 with $k = 3\sigma + 4$ are in bijection with the special closed walks of length d which start in V_1 , in the first step move to V_2 , and from there on visit only vertices in V_0 until they return to the starting vertex from V_1 .

The main thing to note is that the permutation of the sequence (a_i) is reversible, that is, equations 5.24 and 5.25 are satisfied by the original sequence if and only if 5.26 and 5.27 are satisfied by the permuted equation.

The walk initiates on a vertex of the form

$$v_1 = (\alpha', \alpha'', \alpha''', \beta', \beta'', 0, 1)$$

which has a directed edge to all vertices of the form:

$$v_2 = (\alpha'', \alpha''', \alpha^{(4)}, \beta'', \beta^{(3)}, 1, 0)$$

which also satisfy:

$$Y := \alpha' + \alpha''' + \alpha^{(4)} + \beta^{(3)} - 2\beta' \in \{0, 1\}$$

and

$$Z := Y + \alpha' + 1 \in \{0, 1\}$$

as necessitated by 5.32 and 5.33. Until the directed path returns to the vertex v_1 , the last two entries of the vertex vector are both 0. This corresponds to the restriction against having more than one 1 in the same place in a and in $(k-1)a$. The next edge in a walk is between the previous vertex

$$v_2 = (\alpha'', \alpha''', \alpha^{(4)}, \beta'', \beta^{(3)}, 1, 0)$$

and a vertex v_3 of the form

$$v_3 = (\alpha''', \alpha^{(4)}, \alpha^{(5)}, \beta^{(3)}, \beta^{(4)}, 0, 0)$$

which also satisfy:

$$Y := \alpha'' + \alpha^{(4)} + \alpha^{(5)} + \beta^{(4)} - 2\beta'' \in \{0, 1\}$$

and

$$Z := Y + \alpha'' - 2 \in \{0, 1\}.$$

The next $d-3$ directed edges in the circuit are between vertices of the form

$$v_i = (\alpha^{(i)}, \alpha^{(i+1)}, \alpha^{(i+2)}, \beta^{(i)}, \beta^{(i+1)}, 0, 0)$$

and

$$v_{i+1} = (\alpha^{(i+1)}, \alpha^{(i+2)}, \alpha^{(i+3)}, \beta^{(i+1)}, \beta^{(i+2)}, 0, 0)$$

whose entries also satisfy:

$$Y := \alpha^i + \alpha^{(i+2)} + \alpha^{(5)} + \beta^{(4)} - 2\beta'' \in \{0, 1\}$$

and

$$Z := Y + \alpha' \in \{0, 1\}.$$

These last two equations reflect the fact that in the permuted tableau, there is no carry from the i th to $(i + 1)$ st column

By design, if we have a valid sequence originally, the permutation and vertex assignment yield a special closed walk since consecutive vertices satisfy equations 5.28 through 5.33. To show the bijection, we assume that we have a special closed walk in the directed graph and show that this yields a solution a to equation 5.23 which satisfies equations 5.24 and 5.25.

A closed walk commences with an edge

$$\begin{aligned} v_0 &= (\tilde{a}_0, \tilde{a}_1, \tilde{a}_2, \tilde{b}_0, \tilde{b}_1, 0, 1) \in V_1 \\ &\downarrow \\ v_1 &= (\tilde{a}_1, \tilde{a}_2, \tilde{a}_3, \tilde{b}_1, \tilde{b}_2, 1, 0) \in V_2 \end{aligned}$$

satisfying

$$\begin{aligned} \tilde{y}_0 &= \tilde{a}_0 + \tilde{a}_2 + \tilde{a}_3 + \tilde{a}_1 + \tilde{b}_2 - 2\tilde{b}_0 \in \{0, 1\} \\ \tilde{z}_0 &= \tilde{y}_0 + \tilde{a}_0 + 0 + 0 \in \{0, 1\}. \end{aligned}$$

The second edge is of the form

$$\begin{aligned} v_1 &= (\tilde{a}_1, \tilde{a}_2, \tilde{a}_3, \tilde{b}_1, \tilde{b}_2, 1, 0) \in V_2 \\ &\downarrow \\ v_2 &= (\tilde{a}_2, \tilde{a}_3, \tilde{a}_4, \tilde{b}_2, \tilde{b}_3, 0, 0) \in V_3 \end{aligned}$$

satisfying

$$\begin{aligned} \tilde{y}_1 &= \tilde{a}_1 + \tilde{a}_3 + \tilde{a}_4 + \tilde{a}_2 + \tilde{b}_3 - 2\tilde{b}_1 \in \{0, 1\} \\ \tilde{z}_1 &= \tilde{y}_1 + \tilde{a}_1 + 0 - 2 \in \{0, 1\} \end{aligned}$$

and we see that the above edge and equations correspond to the unique place in the string a which satisfies the condition in equation 5.21. The next $2r - 4$ edges in the directed graph are between vertices in V_0 :

$$\begin{aligned} v_i &= (\tilde{a}_i, \tilde{a}_{i+1}, \tilde{a}_{i+2}, \tilde{b}_i, \tilde{b}_{i+1}, 0, 0) \\ &\downarrow \\ v_{i+1} &= (\tilde{a}_{i+1}, \tilde{a}_{i+2}, \tilde{a}_{i+3}, \tilde{b}_{i+1}, \tilde{b}_{i+2}, 0, 0) \end{aligned}$$

satisfying

$$\begin{aligned}\tilde{y}_i &= \tilde{a}_i + \tilde{a}_{i+2} + \tilde{a}_{i+3} + \tilde{a}_{i+1} + \tilde{b}_{i+2} - 2\tilde{b}_i \in \{0, 1\} \\ \tilde{z}_i &= \tilde{y}_i + \tilde{a}_i + 0 + 0 \in \{0, 1\}.\end{aligned}$$

Finally, the edge which closes the closed walk is of the form

$$\begin{aligned}v_{2r-2} &= (\tilde{a}_{2r-2}, \tilde{a}_0, \tilde{a}_1, \tilde{b}_{2r-2}, \tilde{b}_0, 0, 0) \\ &\quad \downarrow \\ v_0 &= (\tilde{a}_0, \tilde{a}_1, \tilde{a}_2, \tilde{b}_0, \tilde{b}_1, 0, 1)\end{aligned}$$

satisfying

$$\begin{aligned}\tilde{y}_{2r-2} &= \tilde{a}_{2r-2} + \tilde{a}_1 + \tilde{a}_2 + \tilde{a}_0 + \tilde{b}_1 - 2\tilde{b}_{2r-2} \in \{0, 1\} \\ \tilde{z}_{2r-2} &= \tilde{y}_{2r-2} + \tilde{a}_{2r-2} + 1 + 0 \in \{0, 1\}.\end{aligned}$$

We will show that the sequence $\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_{2r-2}$ produced by any special closed walk yields a solution to the equations 5.23. $\tilde{x}_j \mapsto x_{(r-1)j}$ is the inverse map of the earlier transformation which took the sequences $\{x_i\}$ to $\{\tilde{x}_j\}$ for $x = a, b, c, y, z$. Under this map, we have

$$\begin{array}{cccc} j & j+2 & j+3 & j+1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ (r-1)j & (r-1)j+2r-2 & (r-1)j+(r-1)-1 & (r-1)j+(r-1) \\ \parallel & \parallel & \parallel & \parallel \\ (r-1)j & (r-1)j-1 & r+(r-1)j-2 & r+(r-1)j-1 \end{array}$$

which implies that the sequence corresponding to a special closed walk in D yields a sequence a with the desired properties.

Let G be a directed multigraph and M the matrix whose i, j entry is the number of directed paths from vertex v_i to vertex v_j . Then the i, j entry in M^2 counts the number of directed walks of length 2 from v_i to v_j . Inductively, the i, j entry in M^r counts the number of directed walks from v_i to v_j . Note that this model is indiscriminate in using an edge multiple times in any directed walk. In particular, the number of closed walks of length r in D is equal to the trace of the matrix M^r .

Recall that $B_{3\sigma+4}$ denotes the number of solutions $a \bmod 2^d - 1$ to equation 5.20 and that $A_{3\sigma+4}(d) = B_{3\sigma+4}(d)/d$. For a fixed $d = 2r - 1$, we can obtain this number of solutions as follows. Let $A_{i,j}$ be the adjacency matrix of the directed graph D restricted to the edges from V_i to V_j for $i, j \in \{0, 1, 2\}$, that is, $A_{i,j}$ is the matrix with rows labeled by the vertices in V_i and the columns labeled by the vertices in V_j , with the entry $(a, b) = 1$ if there is a directed edge from vertex $v_a \in V_i$ to $v_b \in V_j$, and $(a, b) = 0$ otherwise. Then the number of *special* closed walks of length $d = 2r - 1$ is equal to the trace of $A_{1,2}A_{2,0}A_{0,0}^{d-3}A_{0,1}$. By means of the bijection between special closed walks in D and special solutions to equation 5.20, we have the following equation for the generating function for the values of $A_{3\sigma+4}(d)$:

$$\begin{aligned} \sum_{r \geq 2} A_{3,2r+4}(2r-1)z^{r-2} &= \operatorname{tr} \left(\sum_{j=0}^{\infty} A_{1,2}A_{2,0}A_{0,0}^{2j}A_{0,1}z^j \right) \\ &= \operatorname{tr} \left(A_{1,2}A_{2,0} \sum_{j=0}^{\infty} A_{0,0}^{2j}z^j \right) A_{0,1} \\ &= \operatorname{tr}(A_{1,2}A_{2,0}(I - A_{0,0}^2)^{-1}A_{0,1}). \end{aligned}$$

We would like to compute the expression on the right hand side of this equation. Since V_0 is the set of all vertices with $a', a'', a''' \in \{0, 1\}$ and $b', b'' \in \{0, 1, 2, 3\}$, $I - A_{0,0}^2z$ is a 128×128 matrix, which would be difficult to invert with an indeterminate inside. We appeal to the following lemma.

Lemma 5.4.2. *Let $(f_n)_{n \geq 0}$ be a sequence of complex numbers. Suppose that we know that the generating function $\sum_{n \geq 0} f_n z^n$ for the sequence is rational, i.e., that it equals $p(z)/q(z)$ for some polynomials $p(z)$ and $q(z)$ and that the degree of the numerator $p(z)$ is at most P and the degree of the denominator $q(z)$ is at most Q . If the sequence (f_n) satisfies the recurrence*

$$\sum_{i=1}^k a_i f_{n-i} = c$$

for $n = n_0, \dots, N$, where $n_0 \geq k$, $N = \max \{P + k + 1, Q + n_0\}$, and where a_0, a_1, \dots, a_k and c are some given complex numbers, then the recurrence 5.4.2 is satisfied for all $n \geq n_0$.

This is just Theorem 1.8.1

In view of this lemma, we will be done if we can verify the recurrence 5.23 for sufficiently many values of d . On the right side of 5.34, we have a formula which is a rational function in z and we may write the left hand side as $p(z)/q(z)$ where p is a polynomial of degree at most 127 and q is a polynomial of degree at most 128. Taking $n_0 = k = 4$ and $P = 127$, $Q = 128$, we may invoke the preceding lemma, if we can verify the recurrence 5.23 for $d = 11, 13, \dots, 267$. The authors of [EHKX99] did this on a computer. \square

We have now completed a proof of the following.

Corollary 5.4.3. *Let d be an odd integer, $d \geq 3$, and set $\sigma = 2^{(d+1)/2}$. Let $D_{3\sigma+4,d}$ be the $(2^d - 1, 2^{d-1} - 1, 2^{d-2} - 1)$ cyclic quotient set in F_q^* ($q = 2^d$) corresponding to the Glynn hyperoval $D(x^{3\sigma+4})$. Let $\overline{D_{3\sigma+4,d}}$ be the complement of $D_{3\sigma+4,d}$ in F_q^* . Then the 2-rank $B_{3\sigma+4}(d)$ of $\overline{D_{3\sigma+4,d}}$ equals $dA_{3\sigma+4}(d)$, where $A_{3\sigma+4}$ has the first few values given in the Table 5.23 and satisfies the recurrence given in Theorem 5.4.1.*

5.5 The Inequivalence of Certain Difference Sets

At this point we can show that the difference sets arising from translation hyperovals, those arising from the Segre hyperovals $D(x^6)$, and those arising from the Glynn hyperovals $D(x^{3\sigma+4})$ are all distinct.

This follows from the following inequalities whose proofs we leave to the reader:

$$\begin{aligned} A_6(d) &= \frac{2}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{\frac{d+1}{2}} - \left(\frac{1-\sqrt{5}}{2} \right)^{\frac{d+1}{2}} \right) - 1 \\ &< \left(\frac{1+\sqrt{5}}{2} \right)^{\frac{d+1}{2}} \cdot \frac{2}{\sqrt{5}} \\ &< (1.6181)^{\frac{d+1}{2}} < \frac{1}{3} \cdot 2^{\frac{d+1}{2}} < A_{3\sigma+4}. \end{aligned}$$

The last inequality comes from solving the corresponding recurrence (see the original paper for a few hints).

Since the difference sets that arise from translation hyperovals are all Singer sets, we use Theorem 5.1.4 with $p = 2$, $f = 1$, $n = d - 1$, so the 2-rank of the corresponding complementary design is d . For $d \geq 5$ it can be shown that $d < d(2F_{(d-1)/2} - 1) = dA_6(d)$.

Chapter 6

Notes by Carey Jenkins on Theorem 1.5.8

6.1 Solving $S(a)+S(5a)=S(6a)+1$

We wish to describe the solutions mod $2^d - 1$ to the equation $s(a) + s(5a) = s(6a) + 1$ with d a positive integer greater than 1. For brevity, the theorems on the first page are not proven.

Theorem 6.1.1. *Suppose a is an integer such that $0 \leq a < 2^f$ with f a positive integer. Then a has a unique binary representation*

$$a = \sum_{i=0}^{f-1} a_i p^i, \quad a_i \in \{0, 1\}.$$

Example. For $a = 13$ and $f = 4$ we have

$$13 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3.$$

Definition. *Suppose a is an integer such that $0 \leq a < 2^f - 1$. Define the function $S(a)$ by*

$$S(a) = \sum_{i=0}^{f-1} a_i.$$

If a is an integer such that $a \geq 2^f - 1$, then divide a by $2^f - 1$ to get $a = t(2^f - 1) + r$, $0 \leq r < 2^f - 1$, and define $S(a)$ to be $S(r)$.

Example. For $a = 13$ and $f = 4$ we have

$$13 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$$

so that $S(13) = 1 + 0 + 1 + 1 = 3$.

Example. For $a = 22$ and $f = 4$, we have that $22 \bmod (2^4 - 1) = 7$. Then

$$7 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3$$

so that $S(22) = S(7) = 1 + 1 + 1 + 0 = 3$.

Theorem 6.1.2. *Suppose a is reduced modulo $2^f - 1$. Then every cyclic shift of the coefficients of a is given by $2^n \cdot a \bmod 2^f - 1$ for some positive integer n . Furthermore, every $2^n \cdot a \bmod 2^f - 1$ is a cyclic shift of the coefficients, advancing them n times from lower to higher degree terms.*

Example. For $a = 13$, $f = 4$, and 2^3 , we will advance the coefficients three terms. Now

$$a = 13 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$$

so that

$$\begin{aligned} 2^3 13 &= 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 \\ &\equiv 1 \cdot 2^3 + 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 \pmod{2^4 - 1} \\ &= 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3. \end{aligned}$$

Theorem 6.1.3. $S(2a) = S(a)$ for any positive integer a . In particular, this implies that $S(2^n a) = S(a)$ for any positive integer n .

Example. For $a = 13$ and $f = 4$ in the previous example, we know $S(a) = 3$. Now try $2a = 26 \equiv 11 \pmod{2^4 - 1}$.

$$11 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3$$

so that $S(2 \cdot 13) = S(26) = S(11) = 1 + 1 + 1 = 3$ as expected.

Definition. *Suppose a and b are reduced modulo $2^f - 1$. Then let $\begin{bmatrix} a \\ b \end{bmatrix}$ denote the $2 \times f$ matrix having the coefficients of the binary representation of a , written from right to left, in the top row, and similarly the coefficients of b in the bottom row.*

Example. Let $a = 29$ and $b = 21$ with $2^f = 2^5 = 32$. Then

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Definition. In a matrix $\begin{bmatrix} a \\ b \end{bmatrix}$, we call a maximal set of adjacent columns, each column having both entries equal to 1, a J -block and we denote the total number of the columns in all J -blocks by $\sum J$. If we need to make it clear for which matrix $\begin{bmatrix} a \\ b \end{bmatrix}$ we are summing over, we may write $\sum_{\begin{bmatrix} a \\ b \end{bmatrix}} J$.

Example. Consider $\begin{bmatrix} a \\ b \end{bmatrix}$ for $a = 335$ and $b = 204$, $2^f = 512$.

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 0 & \boxed{1} & 0 & 0 & \boxed{1} & \boxed{1} & 1 & 1 \\ 0 & 1 & \boxed{1} & 0 & 0 & \boxed{1} & \boxed{1} & 0 & 0 \end{bmatrix}$$

We see that there are two distinct J -blocks and $\sum J = 3$.

Definition. In a matrix $\begin{bmatrix} a \\ b \end{bmatrix}$, we call a maximal set of adjacent columns, each column having both entries equal to 0, a Z -block.

Example. For the same $\begin{bmatrix} a \\ b \end{bmatrix}$ in the previous example,

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & \boxed{0} & \boxed{0} & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \boxed{0} & \boxed{0} & 1 & 1 & 0 & 0 \end{bmatrix},$$

we see that there there is only one Z -block and it has two columns.

Definition. In a matrix $\begin{bmatrix} a \\ b \end{bmatrix}$, we call a maximal set of adjacent columns, each column having both entries not identical, an A -block. If an A -block is preceded by a J -block (on the right, i.e. AJ), then we call it an A_J -block. Otherwise we call it an A_Z block since it will be preceded by a Z -block. If an A -block is the last block (on the far left) of $\begin{bmatrix} a \\ b \end{bmatrix}$, then if the first block (on the far right) is also an A -block, then we consider both blocks to be one A -block (that wraps around). If the last block on the left is not of type A and the first block on the right is of type A , then the first block is of type A_J if the last block is of type J , else the first block is of type A_Z since the last block is of type Z . We denote the total number of the columns of all A_J -blocks by $\sum A_J$. If we need to make it clear for which matrix we are summing over, we may write $\sum_{\begin{bmatrix} a \\ b \end{bmatrix}} A_J$.

Example. For the same matrix again,

$$\begin{bmatrix} a \\ b \end{bmatrix} = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{array} \right],$$

we see that there is only one A -block (which wraps around). This A -block is of type A_J and $\sum A_J = 4$.

Theorem 6.1.4. *Suppose a and b are reduced modulo $2^f - 1$. Then $s(a+b) = s(a) + s(b) - \sum J - \sum A_J$.*

Proof. We first observe that every $\begin{bmatrix} a \\ b \end{bmatrix}$ has a unique partitioning into blocks of type J , Z , and A . The uniqueness is forced by the maximality with respect to adjacent columns in the definition of these blocks. An inductive approach will prove the theorem. From right to left, we will induct on the appendage of blocks.

For the inductive basis, it is easy to check that the formula is correct for the first block with one subtlety: if the first block is of type A , then for the inductive basis, do not assume it is of type A_J (i.e., assume it is of type A_Z) since we will not use knowledge of the identity of the last block until the inductive step reaches the last block. We will then use a special step to show the formula is correct when appending the last block.

For the inductive step, suppose the sum is correct for the first n blocks:

$$s(a_n + b_n) = s(a_n) + s(b_n) - \sum_{\begin{bmatrix} a_n \\ b_n \end{bmatrix}} J - \sum_{\begin{bmatrix} a_n \\ b_n \end{bmatrix}} A_J.$$

We also assume any carry generated in the sum of the first n blocks is already counted in the formula. Now we append the next block and assume that it is not the last block of $\begin{bmatrix} a \\ b \end{bmatrix}$. We case on block-type.

1. Suppose we append a J -block. We see that in summing the two rows of the J -block, a zero is created in the rightmost summand space, allowing for any incoming carry to be absorbed. Since the incoming carry has already been counted and it has a place to go, it has no effect on our $s(a_{n+1} + b_{n+1})$ summation formula. Now we see that in adding each column of the J -block, two 1's are converted to one 1, as illustrated below.

$$\begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ \hline 1 \leftarrow & 1 & 1 & 1 & 0 \end{array}$$

We see we simply need to subtract the number of columns in this J -block to make the $s(a_{n+1} + b_{n+1})$ count correct. We also observe that the last 1 in the summand is a carry, which as required, is included in the $s(a_{n+1} + b_{n+1})$ count. Also, since we are not appending an A -block, we see that $\sum_{\begin{smallmatrix} [a_n] \\ [b_n] \end{smallmatrix}} A_J = \sum_{\begin{smallmatrix} [a_{n+1}] \\ [b_{n+1}] \end{smallmatrix}} A_J$. Thus we have

$$s(a_{n+1} + b_{n+1}) = s(a_{n+1}) + s(b_{n+1}) - \sum_{\begin{smallmatrix} [a_{n+1}] \\ [b_{n+1}] \end{smallmatrix}} J - \sum_{\begin{smallmatrix} [a_{n+1}] \\ [b_{n+1}] \end{smallmatrix}} A_J$$

as desired.

2. Suppose we append a Z -block. When adding the rows of a Z -block, again a zero is created in the rightmost summand space, allowing for a carry (already counted) to be absorbed.

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}$$

Since the Z -block has no ones and generates no ones, appending it has no effect on the formula so we have

$$s(a_{n+1} + b_{n+1}) = s(a_{n+1}) + s(b_{n+1}) - \sum_{\begin{smallmatrix} [a_{n+1}] \\ [b_{n+1}] \end{smallmatrix}} J - \sum_{\begin{smallmatrix} [a_{n+1}] \\ [b_{n+1}] \end{smallmatrix}} A_J.$$

3. Suppose we append an A -block. We have two possibilities: A_Z or A_J .

- (a) If the preceding block was of type Z , there is no incoming carry and we observe that in adding the rows of the A -block, there is no generation nor absorption of any 1's.

$$\begin{array}{cccc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 \end{array}$$

Precisely these 1's will be converted to 0's when we add the carry, and then the carry is absorbed by the first zero after these 1's. This carry has already been counted as desired. We now correctly reclassify the first A -block as type A_J and subtract the A_J columns (after subtracting the last J columns if there were any) and we have the correct count. \square

Some examples are in order.

Example.

$$\left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ \hline 1 \leftarrow & 0 & 0 & 0 & 1 & 1 \end{array} \right]$$

Reducing the sum modulo $2^f - 1$, it equals $(000100)_2$ so that $s(a+b) = 1$. Here we see that the last A_J wraps around and that its carry annihilates the 1's under the wrap-around. Our theorem gives

$$\begin{aligned} s(a+b) &= s(a) + s(b) - \sum J - \sum A_J \\ &= 5 + 2 - 1 - 5 = 1. \end{aligned}$$

Example.

$$\left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ \hline 1 \leftarrow & 1 & 1 & 0 & 0 & 1 & 1 \end{array} \right]$$

Reducing the sum modulo $2^f - 1$, it equals $(110100)_2$ so that $s(a+b) = 3$. Here we see that the last block is of type J and has a carry which annihilates the 1's under the first block which is of type A_J . Our theorem gives

$$\begin{aligned} s(a+b) &= s(a) + s(b) - \sum J - \sum A_J \\ &= 5 + 4 - 3 - 3 = 3. \end{aligned}$$

Theorem 6.1.5. *Fix modulus $2^f - 1$. Then a is a solution to $s(a) + s(5a) = s(6a) + 1$ if and only if the matrix $\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}$ has exactly one J -block and this J -block has exactly one column and this column is followed immediately by a Z -block.*

Proof. Using properties of modular arithmetic, the fact that $S(a) = S(r)$, and Theorem 6.1.4, we have

$$\begin{aligned}
s(6a) &= s(a + 5a) \\
&= s((a + 5a) \bmod 2^f - 1) \\
&= s(((a \bmod 2^f - 1) + (5a \bmod 2^f - 1)) \bmod 2^f - 1) \\
&= s((a \bmod 2^f - 1) + (5a \bmod 2^f - 1)) \\
&= s(a \bmod 2^f - 1) + s(5a \bmod 2^f - 1) \\
&\quad - \sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} J - \sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} A_J \\
&= s(a) + s(5a) - \sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} J - \sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} A_J
\end{aligned}$$

Thus a is a solution to $s(a) + s(5a) = s(6a) + 1$ if and only if

$$\sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} J + \sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} A_J = 1 \tag{6.1}$$

Now both $\sum J$ and $\sum A_J$ are nonnegative, and $\sum A_J > 0$ implies that $\sum J > 0$ so we have Equation 6.1 if and only if $\sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} J = 1$ and $\sum_{\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}} A_J = 0$. This condition is equivalent to the one in the statement of the theorem, so we are done. \square

A technical note: The definition of $\begin{bmatrix} a \\ b \end{bmatrix}$ requires that a and b be reduced modulo $2^f - 1$. This is why a and $5a$ must be reduced in the expression $\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}$. Theorem 6.1.4 implicitly assumes this reduction. The reduction of $5a$ plays a critical part in the upcoming arguments.

Now we are ready to prove the main theorem.

Theorem 6.1.6. *Let $d \geq 2$ be an integer. The binary representations of the solutions $a \bmod 2^d - 1$ to the equation $s(a) + s(5a) = s(6a) + 1$ are constructed by the following algorithm.*

1. Form all possible binary strings of length at most d by concatenating blocks of the form 01, 0011, 00111 subject to the following restrictions.

- (a) In a string having length less than d , the rightmost block must be 01 and the block 00111 must not occur.
- (b) In a string having length equal to d , the block 00111 must occur exactly once and as the rightmost block.
2. Given a string of length k constructed in Step 1, append $d - k$ many 0's on the left to form a string of length d .
3. The binary representations of the set of solutions reduced modulo $2^d - 1$ consist of all possible rotations of the string constructed in Step 2.

Proof. The proof has two major parts. First, we show that all strings formed by the algorithm are indeed solutions. Second, we show that any string not constructed by the algorithm above is not a solution.

In our work, we will construct $\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}$ and see if the necessary and sufficient condition of Theorem 6.1.4 is satisfied or violated. In the construction of $\begin{bmatrix} a \bmod 2^f - 1 \\ 5a \bmod 2^f - 1 \end{bmatrix}$, we will insert a row for $4a$ inbetween the rows for a and $5a$ so that we may compute $5a \bmod 2^f - 1$ by adding the a row and the $4a$ row. The row $4a$ will be reduced modulo $2^f - 1$ by use of Theorem 6.1.2, i.e., it will consist of a cyclically advanced two entries. Then in computing $5a$, since it must be reduced modulo $2^f - 1$ in order to apply Theorem 6.1.4, we will always watch for a wrap-around carry. Therefore, to simplify notation, we will no longer write “mod $2^d - 1$ ” since all computations will be reduced $2^d - 1$ henceforth.

We first justify Step 3. From Theorem 6.1.2, we know that any cyclic shift of a number a is equivalent to multiplying it by 2^k for some positive integer. k . From Theorem 6.1.3, we know that $s(a)$ and $s(2^k a)$ are equal. Therefore, for any cyclic shift $2^k a$ of a ,

$$s(a) + s(5a) = s(2^k a) + s(2^k(5a)) = s(2^k a) + s(5(2^k a))$$

and

$$s(6a) + 1 = s(2^k(6a)) + 1 = s(6(2^k a)) + 1$$

so that

$$\begin{aligned} s(a) + s(5a) &= s(6a) + 1 \\ \Leftrightarrow s(2^k a) + s(5(2^k a)) &= s(6(2^k a)) + 1. \end{aligned}$$

Thus we have shown that a is a solution if and only if a cyclic shift of a is a solution.

Now let us show that Steps 1 and 2 of the algorithm give solutions. Let us address the case in which $k < d$. So we have at least one zero appended to the end of the string by Step 2. Prior to this last zero we must have another zero either from Step 2 or from a previous 01 or 0011 block. From Step 1, our first block is 01. So we observe that by construction, we have the $\begin{bmatrix} a \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ required by Theorem 6.1.2:

$$\left[\begin{array}{cccccc} 0 & 0 & \dots & & 0 & 1 & : a \\ & & & & \dots & 0 & 1 & 0 & 0 & : 4a \\ \hline & & & & \dots & & & 0 & 1 & : 5a \end{array} \right].$$

But what if there is a wrap-around carry to be accounted for in computing $5a$? We now show this is not possible. If there is a carry, then we must have a 1 as the last entry of the $4a$ row implying that the last block of the a row is 01 (in bold below) which by construction will be preceded by a 0:

$$\left[\begin{array}{cccccc} 0 & \mathbf{0} & \mathbf{1} & 0 & \dots & 0 & 1 & : a \\ 1 & 0 & & & \dots & 0 & 0 & : 4a \\ \hline 1 & & & & \dots & 0 & 1 & : 5a \end{array} \right].$$

Thus we have a Z -block having one column in $\begin{bmatrix} a \\ 4a \end{bmatrix}$ blocking any carries from reaching the last 1 in the $4a$ row. Thus there is no wrap-around carry in the sum $5a$.

To finish the case $k < d$, we must show that no other $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$'s are generated by further appendage of 01 and 0011 blocks.

We will subcase on 01|01, 0011|01, 0011|0011, and 01|0011 and show that in each instance, no further $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is contributed to $\begin{bmatrix} a \\ 5a \end{bmatrix}$. In this strategy, we only look for $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in the overlapping entries of the a and $4a$ rows, for every column of $\begin{bmatrix} a \\ 5a \end{bmatrix}$ consists of such overlapping entries.

1. Case 01|01. First suppose there is no carry coming in from the right above the bold entry:

$$\left[\begin{array}{cccccc} \dots & & 0 & \mathbf{1} & 0 & 1 & \dots & : a \\ \dots & 0 & 1 & 0 & 1 & & \dots & : 4a \\ \hline \dots & & & 1 & 0 & & \dots & : 5a \end{array} \right].$$

Then we see that no $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is generated in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ as desired. Now suppose there is a carry coming in from the right above the bold entry:

$$\left[\begin{array}{cccccccc} \dots & & 0 & \mathbf{1} & 0 & 1 & \dots & : a \\ \dots & 0 & 1 & 0 & 1 & & \dots & : 4a \\ \hline \dots & & 0 & 1 & & & \dots & : 5a \end{array} \right].$$

Then we see that a $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is generated, but for this carry to arise, there must be a 1 (boxed) in the $4a$ row which means it must also be in the a row as well (boxed):

$$\left[\begin{array}{cccccccc} \dots & & 0 & \mathbf{1} & 0 & 1 & \boxed{1} & \dots & : a \\ \dots & 0 & 1 & 0 & 1 & \boxed{1} & & \dots & : 4a \\ \hline \dots & & 0 & 1 & & & & \dots & : 5a \end{array} \right].$$

But then we have a block 011 which is not possible by the construction. So we are done.

2. Case 0011|01. (This follows the same argument as the previous case.) First suppose there is no carry coming in from the right above the bold entry:

$$\left[\begin{array}{cccccccc} \dots & & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 1 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 0 & 1 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 0 & & & \dots & : 5a \end{array} \right].$$

Then we see that no $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is generated in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ as desired. (For Case 3 below, we will need the observation here that a carry is passed along to the left.) Now suppose there is a carry coming in from the right above the bold entry:

$$\left[\begin{array}{cccccccc} \dots & & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 1 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 0 & 1 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & & & \dots & : 5a \end{array} \right].$$

Then we see that a $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is generated, but for this carry to arise, there must be a 1 (boxed) in the $4a$ row which means it must also be in the

a row as well (boxed):

$$\left[\begin{array}{cccccccc|c} \dots & & 0 & 0 & 1 & \mathbf{1} & 0 & 1 & \boxed{1} & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 0 & 1 & \boxed{1} & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & & & & \dots & : 5a \end{array} \right].$$

But then we have a block 011 which is not possible by the construction. So we are done.

3. Case 0011|0011. Appending an 0011 to an 0011 creates a different scenario. If we have an incoming carry to the bold entry,

$$\left[\begin{array}{cccccccc|c} \dots & & 0 & 0 & 1 & 1 & \mathbf{0} & 1 & 1 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 0 & 0 & 0 & & \dots & : 5a \end{array} \right],$$

then no $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is generated in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ as desired. Now in any chain 0011|0011|...|0011|01 there must be a first 01 which will precisely give us the desired carry as observed in Case 2 above.

4. Case 01|0011. In this case, as in Case 3 above, we are assured of an incoming carry since the 0011 on the right will be part of a 0011|...|0011|01 chain. Then we have

$$\left[\begin{array}{cccccc|c} \dots & & 0 & 1 & 0 & \mathbf{0} & 1 & 1 & \dots & : a \\ \dots & 0 & 1 & 0 & 0 & 1 & 1 & & \dots & : 4a \\ \hline \dots & & 1 & 0 & 0 & 0 & & & \dots & : 5a \end{array} \right],$$

with no $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ as desired.

So we have shown that all string generated in Steps 1 and 2 having length k less than d are solutions as desired. Now we wish to show that the strings having length $k = d$ constructed in Step 1 are also solutions.

First, we can see that 00111 is a solution (with no 01 and 0011 blocks appended):

$$\left[\begin{array}{cccccc|c} & & 0 & 0 & 1 & 1 & 1 & : a \\ & & 1 & 1 & 1 & 0 & 0 & : 4a \\ \hline 1 \leftarrow & & 0 & 0 & 0 & 1 & 1 & \\ \equiv & & 0 & 0 & 1 & 0 & 0 & : 5a \end{array} \right].$$

Now things become a bit tricky. Some observations are needed.

Observation 1. When appending $0011|0011|\dots|0011$ strings (even those with one 0011 block), they *always* pass a carry. The proof comes from the fact that each of these strings must either be preceded by a 01 block or the original 00111 block. We check both cases.

Suppose a $0011|0011|\dots|0011$ string is preceded by a 01 block. Then we see that in $\begin{bmatrix} a \\ 4a \end{bmatrix}$ there is a J -block (in bold) generating a carry and that this carry is passed along:

$$\left[\begin{array}{cccccccc} 1 \leftarrow & & & & & & & & \\ & 0 & 0 & 1 & \mathbf{1} & 0 & 1 & & : a \\ 0 & 0 & 1 & 1 & 0 & \mathbf{1} & & & : 4a \\ \hline & & 0 & 0 & 0 & & & & : 5a \end{array} \right].$$

Appending more 0011 blocks above simply keeps moving the carry along.

Now suppose a $0011|0011|\dots|0011$ string is preceded by the original 00111 block. Again a J -block (in bold) in $\begin{bmatrix} a \\ 4a \end{bmatrix}$ guarantees the generation of a carry:

$$\left[\begin{array}{cccccccc} 1 \leftarrow & & & & & & & & \\ & 0 & 0 & 1 & 1 & 0 & 0 & \mathbf{1} & 1 & 1 & : a \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \mathbf{1} & & : 4a \\ \hline & & 0 & 0 & 0 & 0 & 0 & 0 & & & : 5a \end{array} \right].$$

So now we know that whenever we see a $0011|0011|\dots|0011$ string, a carry is passed along.

Observation 2. No $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$'s are generated in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ in the overlapping entries of 0011 blocks. This is easily seen by examining the diagrams in Observation 1.

Observation 3. $01|01|\dots|01$ strings (including the one with a single block) always kill an incoming carry and then generate a new one. Observe that the 01 block must be preceded by a 0 and followed by a 1 so we have the following:

$$\left[\begin{array}{cccccccc} \dots & & \mathbf{1} & \mathbf{0} & 1 & 0 & \dots & : a \\ \dots & 1 & 0 & \mathbf{1} & \mathbf{0} & & \dots & : 4a \\ \hline \dots & & 0 & ? & & & \dots & : 5a \end{array} \right].$$

To prove this observation, we see that there is a Z -block in $[\begin{smallmatrix} a \\ 4a \end{smallmatrix}]$ to kill the incoming carry and it is immediately followed by a J -block that generates a carry. These are in bold above.

Observation 4. As can be seen in the diagram above, no $[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}]$'s are generated in $[\begin{smallmatrix} a \\ 5a \end{smallmatrix}]$ in the overlapping entries of 01 blocks.

Observation 5. In the overlapping entries of 01 and 0011 blocks, no $[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}]$'s occur in $[\begin{smallmatrix} a \\ 5a \end{smallmatrix}]$. We check both cases, first, 0011|01:

$$\left[\begin{array}{cccccccccc} \dots & & 0 & 0 & 1 & 1 & 0 & 1 & 0 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 0 & 1 & 0 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 0 & ? & & & \dots & : 5a \end{array} \right],$$

which is fine, and also 01|0011 (recall 0011 is passing a carry to the bold entry):

$$\left[\begin{array}{cccccccccc} \dots & & 0 & 1 & 0 & \mathbf{0} & 1 & 1 & \dots & : a \\ \dots & 0 & 1 & 0 & 0 & 1 & 1 & & \dots & : 4a \\ \hline \dots & & 1 & 0 & 0 & 0 & & & \dots & : 5a \end{array} \right].$$

Now we can put these observations together to prove the remaining constructions are solutions in the case $k = d$. Here is an outline of what happens next:

1. We show 0011|0011|...|0011|00111 is a simple solution.
2. Replace arbitrarily many 0011's, except the last, with 01 to get more solutions that are the same "under" 00111.
3. Now redo Case 2 above, but let the last block be 01 and see that we get a different sort of solution under 00111.

Thus we will have shown that all strings generated by the $k = v$ case are solutions.

1. 0011|0011|...|0011|00111.

$$\left[\begin{array}{cccccccccccc} 0 & 0 & 1 & 1 & \dots & & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & : a \\ 1 & 1 & & & \dots & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & : 4a \\ \hline 1 \leftarrow & 0 & 0 & & \dots & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \\ \equiv & 0 & 0 & & \dots & & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & : 5a \end{array} \right]$$

2. $0011|\dots$ any $\dots|00111$. Since the string ends at the far left with 0011, we know from Observation 1 that a 1 will be passed around to give the same solution configuration at the far right under 00111 as in Case 1 above. Inbetween the last 0011 and first 00111, we know from Observations 2, 4, and 5 that no additional $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$'s are generated. So these are solutions.
3. $01|\dots$ any $\dots|00111$. Again, we know that inbetween the first 00111 and last 01, everything is fine, but we have a different $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ configuration (notice carry-killing Z -block at far left in $\begin{bmatrix} a \\ 4a \end{bmatrix}$ helps out):

$$\left[\begin{array}{cccccccc|c} 0 & 1 & \dots & & 0 & 0 & 1 & 1 & 1 & : a \\ 0 & & \dots & 0 & 0 & 1 & 1 & 1 & 0 & 1 & : 4a \\ \hline & & \dots & & 0 & 0 & 1 & 0 & 0 & & : 5a \end{array} \right].$$

So we have finished the main section showing that the strings constructed by the algorithm are solutions. Now we must determine what strings have not been constructed and show that each of these is not a solution. In Stan's notes, we have eliminated all strings containing 1111, 111 not preceded by 00, and 11 not preceded by 00. The strings remaining to be eliminated are outlined below.

1. Strings having more than one location of inserted zeros (zeros not part of 01, 0011, or 00111).
 2. Strings having more than one 00111.
 3. In $k < d$ case, strings beginning with 0011.
 4. In $k < d$ case, strings having 00111.
 5. In $k = d$ case, strings not having 00111.
1. To show that no string may have more than one location of inserted zeros (those not part of a 01, 0011, or 00111 block), we will show that a $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ occurs in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ for each such location. We will case on the block preceding the inserted zeros.

First suppose an inserted zero is preceded by 0011. Here we will see that in $\begin{bmatrix} a \\ 4a \end{bmatrix}$ we have a Z -block (boxed) absorbing carries, thus guaranteeing

the generation of $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ under the first 1 that follows the inserted zeros:

$$\begin{bmatrix} \dots & \dots & \boxed{0} & 0 & 0 & 1 & 1 & \dots & : a \\ \dots & 0 & 0 & \boxed{0} & 1 & 1 & \dots & & : 4a \end{bmatrix}.$$

You may ask, “What if there is a wrap-around carry in row $5a$ to upset this $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$?” This cannot happen. For a wrap-around carry to reach the $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$, we must have a 1 under the Z -block boxed above and 1’s under the A -block before it. But this is a contradiction since the A -block would have to pass a carry to put the 1 under the Z -block, in which case the A -block would have 0’s underneath. [Illustrated below in next case.]

Now suppose an inserted zero is preceded by 01. To avoid the 0011 case, we must precede the 01 block by a 0 (bold): [To make this argument precise: if we do not have this 0, then we have a 011. 011’s are not legal without a second preceding 0. Thus we have a 0011. We have already analyzed 0011 above.]

$$\begin{bmatrix} \dots & \dots & 0 & 0 & 1 & \mathbf{0} & \dots & : a \\ \dots & 0 & 0 & 1 & 0 & & \dots & : 4a \end{bmatrix}.$$

As in the 0011 case, the Z -block in $\begin{bmatrix} a \\ 4a \end{bmatrix}$ blocks carries. So we know that the first 1 following the inserted zeros will have a 1 underneath in row $5a$ as desired. Now we must consider the effect of a wrap-around carry in row $5a$. Consider the necessary configuration for the carry to reach (and thus upset) the $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$:

$$\begin{bmatrix} 1 & \dots & & 0 & 0 & 1 & 0 & \dots & : a \\ 0 & \dots & 0 & 0 & 1 & 0 & & \dots & : 4a \\ \hline 1 & \dots & 1 & \boxed{1} & 1 & 1 & & : 5a \end{bmatrix}.$$

Again, as in the 0011 case above, the boxed 1 cannot exist and have 1’s under the preceding A -block of $\begin{bmatrix} a \\ 4a \end{bmatrix}$ simultaneously. Thus a wrap-around carry cannot upset the $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ as desired.

Now suppose an inserted zero is preceded by 00111. In Case 2 below, we will show that every occurrence of 00111 does exactly one of the following: the 00111 generates a $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ or the 00111 causes a failure of the necessary and sufficient criterion of Theorem 6.1.5.

So given acceptance of Case 2 below, we are done with Case 1 and conclude that no two locations may have inserted zeros.

2. We will now show that no string may have more than one 00111. Our strategy is to show that each instance of 00111 forces a $\boxed{1}$ in $[\frac{a}{5a}]$ (thus not allowing more than one 00111) or does not meet the criterion of Theorem 6.1.5. We will begin by casing on whether the boxed entry below receives a carry or not. First, assume it receives a carry:

$$\left[\begin{array}{cccccccc} & & & & 1 & & & \\ \dots & & 0 & 0 & 1 & \boxed{1} & 1 & 0 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 1 & 0 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 1 & 0 & & & \dots & : 5a \end{array} \right].$$

Then we have our $\boxed{1}$ in $[\frac{a}{5a}]$ that cannot be upset by a wrap-around carry since in row $5a$, it is preceded by a 0.

Now suppose the boxed entry receives no carry:

$$\left[\begin{array}{cccccccc} & & & & 0 & & & \\ \dots & & 0 & 0 & 1 & \boxed{1} & 1 & 0 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 1 & 0 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & & & \dots & : 5a \end{array} \right].$$

You may say, “We have an illegal configuration in $[\frac{a}{5a}]$, thus this is not allowed.” But it is not that simple. A wrap-around carry in row $5a$ can fix the problem as shown in the sole 00111 solution to the $k = d$ case. So further investigation is required. To stay in this case, we require a second 0 to the right (else we have the carry):

$$\left[\begin{array}{cccccccc} & & & & 0 & & & \\ \dots & & 0 & 0 & 1 & 1 & 1 & 0 & 0 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 1 & 0 & 0 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & & & \dots & : 5a \end{array} \right].$$

We must show there is no possibility of a wrap-around salvation of the above illegal configuration (at least no salvation without putting

To keep 1's in row $5a$ as required to pass the wrap-around carry, we need more A -blocks in $[\frac{a}{4a}]$. We put the required 1's in row $5a$ below to help us visualize:

$$\left[\begin{array}{cccccccccccccccc} \dots & & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & & & \dots & : 5a \end{array} \right].$$

This new string of 0011's in row a cannot be preceded by any of 01, 00111, or 000 and maintain consecutive 1's in row $5a$. We show each possibility below without comment. First, 01:

$$\left[\begin{array}{cccccccccccccccc} \dots & & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & & & \dots & : 5a \end{array} \right].$$

Second, 00111:

$$\left[\begin{array}{cccccccccccccccc} \dots & & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & \dots & : 5a \end{array} \right].$$

Now, 000:

$$\left[\begin{array}{cccccccccccccccc} \dots & & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & \dots & : a \\ \dots & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & & \dots & : 4a \\ \hline \dots & & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & & \dots & : 5a \end{array} \right].$$

We have done it. We have shown that no string may have two 00111 blocks.

3. Suppose $k < d$, and our string begins with 0011. Since we have shown there can only be one location of inserted zeros and every cyclic advance of a solution is a solution, we may assume that the 0011 is at the far right and the inserted zeros are at the far left. We case on a carry into

Since it is the first block of the string, we must also have these zeros (one inserted, the other inserted or part of a block):

$$\left[\begin{array}{cccccccc|c} 0 & 0 & \dots & & 0 & 0 & 1 & \boxed{1} & 1 & : a \\ & & \dots & 0 & 0 & 1 & 1 & 1 & 0 & 0 : 4a \\ \hline & & \dots & & 0 & 0 & 1 & 0 & & : 5a \end{array} \right].$$

For this carry to be possible, we must have 1's under these zeros to pass the carry along at the far left of row $4a$:

$$\left[\begin{array}{cccccccc|c} & & & & & & & & 1 & \\ 0 & 0 & 1 & 1 & \dots & & 0 & 0 & 1 & \boxed{1} & 1 & : a \\ 1 & 1 & & & \dots & 0 & 0 & 1 & 1 & 1 & 0 & 0 : 4a \\ \hline & & & & \dots & & 0 & 0 & 1 & 0 & & : 5a \end{array} \right].$$

Since we have 0011 at the far left in row a , this contradicts that 00111 begins the string.

- (c) Now suppose the first block is 01. By Case 2, we know that if a is a solution, then the later 00111 will generate a $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$. We will now show that the first 01 will also generate $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$, thus violating the criterion of Theorem 6.1.5. First observe that since 01 begins the string, we must have these zeros at the far left (one inserted, the other inserted or part of a block):

$$\left[\begin{array}{cccc|c} 0 & 0 & \dots & 0 & 1 & : a \\ & & \dots & 0 & 1 & 0 & 0 : 4a \\ \hline & & \dots & & & : 5a \end{array} \right].$$

With no incoming carry, we immediately see the $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ under the first column. So we ask, "Is it possible for a carry to wrap around?" The answer is no as it would require 1's under these 0's to pass the carry, thus placing a 0011 block at the far left and contradicting 01 beginning the string:

$$\left[\begin{array}{cccc|c} 0 & 0 & 1 & 1 & \dots & 0 & 1 & : a \\ 1 & 1 & & & \dots & 0 & 1 & 0 & 0 : 4a \\ \hline & & & & \dots & & & : 5a \end{array} \right].$$

We conclude that if $k < d$, no 00111 may be present.

5. Now in the case that $k = d$ we finish the theorem by showing that 00111 must be present. Note that this will imply that solutions for $k = d$ exist if and only if d is odd since 00111 cannot occur more than once, 00111 has an odd number of digits, and 01 and 0011 have an even number of digits. For sake of contradiction, suppose a is a solution and 00111 is not in a . Then we only have 01 and 0011 blocks in the string. One can easily see by sketching a diagram that a string consisting of only 0011's is not a solution, nor is a string consisting only of 01's. So now we consider strings having both 01's and 0011's.

Now take any string of mixed 01's and 0011's, and without loss of generality, cycle the string until a 0011 is at the far right and the left-most block is 01. Then we have a carry from the first column causing zeros in row $5a$:

$$\left[\begin{array}{cccccccc} 0 & 1 & \dots & & 0 & 0 & 1 & 1 & : a \\ & & & \dots & 0 & 0 & 1 & 1 & 0 & 1 & : 4a \\ \hline & & & & & & 0 & 0 & 0 & 0 & : 5a \end{array} \right]$$

We observe from the diagram above that a wrap-around carry can only effect the first entry of row $5a$ and in fact would cause an illegal configuration in the first two columns of $\begin{bmatrix} a \\ 5a \end{bmatrix}$. Now we observe the carry passed by the A_J block of $\begin{bmatrix} a \\ 4a \end{bmatrix}$ will eventually reach a 01 in row a and have no ill effect. We show this in the diagram below, and as usual, draw only one 0011 to represent a possibly greater string of 0011's:

$$\left[\begin{array}{cccccccc} 0 & 1 & \dots & & 0 & 1 & 0 & 0 & 1 & 1 & : a \\ & & & \dots & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & : 4a \\ \hline & & & & & & 1 & 0 & 0 & 0 & 0 & 0 & : 5a \end{array} \right]$$

Now we observe that any additional 01's has no ill effect, nor produces the desired $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $\begin{bmatrix} a \\ 5a \end{bmatrix}$, and then the argument repeats. In other words, this string of 01's must finally meet an 0011, and the pattern above reiterates. $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is never generated in $\begin{bmatrix} a \\ 5a \end{bmatrix}$ so that this is not a solution. And as mentioned earlier, any wrap-around carry definitely creates a

non-solution via an illegal configuration. We show the pattern below without further comment.

$$\left[\begin{array}{cccccccccccc|c} 0 & 1 & \dots & & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & : & a \\ & & \dots & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & : & 4a \\ \hline & & & & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & : & 5a \end{array} \right]$$

$$\left[\begin{array}{cccccccccccc|c} 0 & 1 & \dots & & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & : & a \\ & & \dots & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & : & 4a \\ \hline & & & & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & : & 5a \end{array} \right]$$

This concludes the last case of the second part of the theorem. Thus the theorem is proven.

□

For the record, we restate an observation of the last case of the preceding theorem.

Corollary 6.1.7. *If k is the length of the of string of 01's, 0011's, and 00111's constructed in the algorithm of Theorem 6.1.6 and $k = d$, then $a \bmod 2^d - 1$ is a solution of $s(a) + s(5a) = s(6a) + 1$ if and only if d is odd.*

Bibliography

- [EHKX99] R. Evans, H. Hollmann, C. Krattenthaler and Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *Jour. Comb. Theory. (A)* 87(1999), 74 – 119.
- [Gl83] D. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, Combinatorial mathematics, X(Adelaide, 1982), 217 – 229, *Lecture Notes in Math.*, 1036, Springer, Berlin, 1983.
- [IR93] Ireland and Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, Springer-Verlag, 1993.
- [Ma98] A. Maschietti, Difference sets and hyperovals, *Designs, Codes and Crypt.*, 14 (1998), 89 – 98.
- [Pa05] S. E. Payne, *Topics in Finite Geometry: Ovals, Ovoids and Generalized Quadrangles*, in preparation.
- [PT84] S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles*, Pitman, Research Monograph #110, 1984.
- [Ri01] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.
- [Ry63] H. Ryser, *Combinatorial Mathematics*, Carus Monograph No. 14, MAA, 1963.
- [Sc03] B. Schmidt, *title*, Springer, 2003.

- [VLW96] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1996.

Index

- $A_k(f)$, 26, 31
- $B_k(f)$, 26
- $D_{k,q}$, 99
- $L(x)$, 23
- $S(a)$, 23
- $\Phi(P)$, 77
- \hat{G} , 7
- $\langle u \rangle$, 24
- $[u]$, 24
- $\tilde{s}(a)$, 85
- $g(P)$, 77
- g_a , 84
- σ_a , 65

- additive character, 74
- augmentation map, 19

- character of finite abelian group, 7
- Chinese Remainder Theorem, 59
- class number, 54
- cyclotomic coset, 104
- cyclotomic field, 63

- decomposition group, 68
- degree of a prime ideal, 59
- difference set, 15
- discriminant of basis, 45

- equivalent difference sets, 18

- floor function, 24
- fractional part, 24

- Gauss sum, 77
- Glynn hyperovals, 34
- group ring, 18

- Hall multiplier, 41
- hyperoval, 33

- integral basis, 52

- Jacobi sum, 80

- Lagrange interpolation, 11

- maximal ideal, 53
- multiplicative character, 74
- multiplier of quotient set, 41

- Noetherian ring, 53
- norm, 10

- ord_P , 57
- orthogonality relations, 8
- oval, 33

- prime ideal, 53
- primitive element, 9
- principal character, 7

- quotient set, 16

- ramification index of a prime ideal, 58
- rational generating function, 35
- regular hyperoval, 34

Segre hyperoval, 34
Singer difference sets, 93
symmetric block design, 13

Teichmüller character, 83
trace, 10
transfer matrix method, 35
translation hyperoval, 34