Fourier transform in cyclic groups

Yves Benoist

Abstract

On a cyclic group of prime order, the non-trivial Dirichlet characters together with their Fourier transform have constant modulus outside 0 and vanish at 0. Answering a question of H. Cohn, we construct new functions with these properties. The proof relies on Floer homology. We also apply this method to the *biunimodular functions problem*.

Contents

1 Introduction **2**
- 1.1 The Harvey Cohn's problem 3
- 1.2 Main results 4
- 1.3 Biunimodular functions 5
- 1.4 Organization 5

2 Using Symplectic Geometry **6**
- 2.1 The unitary group 6
- 2.2 The finite Fourier transform 7
- 2.3 Existence of unimodular $\mathcal{C}$-functions 8

3 Equivariant unimodular $\mathcal{C}$-functions **9**
- 3.1 The Jacobi sums 9
- 3.2 Equivariant $\mathcal{C}$-functions 11
- 3.3 Transversality of Clifford tori 12
- 3.4 Unimodular $\mathcal{C}$-functions for non safe prime 14

2020 Math. subject class. Primary 11F03 ; Secondary 11F27

Key words Finite Fourier transform, Cyclic group, Floer homology, Jacobi sums, Stickelberger formula, Biunimodular vectors.

4 Using cyclotomic field theory **16**
4.1 Action on $(\mathbb{Z}/d\mathbb{Z})^2$ 17
4.2 The Stickelberger's formula 21
4.3 Distinguishing Jacobi sums 21
4.4 Example of equalities between Jacobi sums 22

5 Unimodular $\mathcal{C}$-functions for safe primes **24**
5.1 Strategy 24
5.2 A quadratic functional equation 26
5.3 Multiplicity of holomorphic maps 27
5.4 Multiplicity of $T \cap F^{-1}T$ at the Legendre character 29
5.5 Moving slightly the torus 31

6 Counting $\mathcal{C}$-functions **35**
6.1 Finiteness of the set of $\mathcal{C}$-functions 35
6.2 Counting equivariant $\mathcal{C}$-functions 37

7 Examples **41**
7.1 When $d = 7$ 41
7.2 When $d = 9$ 41
7.3 When $d = 11$ 42
7.4 When $d = 13$ 44

A Appendix: Biunimodular functions **45**
A.1 Classical biunimodular functions 45
A.2 Constructing biunimodular functions 46
A.3 Transversality at gaussian functions 47
A.4 Transversality at Björck functions 49

1 Introduction

The starting point of this article is the following problem asked by Harvey Cohn in 1994 which is Problem 39 p. 202 in [27]. The first aim of this article is to give an answer to this problem. The proof will rely not only on tools coming from Cyclotomic Field Theory but also on tools coming from Floer Homology.

1.1 The Harvey Cohn's problem

This problem is looking for a converse of a well-known property of the Dirichlet characters which, by definition, are the characters of the multiplicative group $\mathbb{F}_p^*$ of the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We recall that a character $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ is a map such that $\chi(k\ell) = \chi(k)\chi(\ell)$ for all k, ℓ in $\mathbb{F}_p^*$. We extend χ to $\mathbb{F}_p$ by setting $\chi(0) = 0$. When χ is non trivial, these functions χ satisfy Condition (1.1) below. More generally, we will also deal with cyclic groups $C_d := \mathbb{Z}/d\mathbb{Z}$ of odd order d.

Definition. A function f on the cyclic group C_d vanishing at 0 and satisfying the condition

$$\sum_{k \in C_d \smallsetminus \{0\}} f(k-\ell)\ f(k)^{-1} \ = \ -1 \quad \text{for } \ell \neq 0. \tag{1.1}$$

will be called a $\mathcal{C}$-function.

Definition. A function $f : C_d \to \mathbb{C}$ such that $f(0) = 0$ is said to be *unimodular on* $C_d \smallsetminus \{0\}$ if $|f(\ell)| = 1$ for $\ell \neq 0$.

When f is a $\mathcal{C}$-function we will say *a unimodular $\mathcal{C}$-function* as a shortcut for *a $\mathcal{C}$-function that is unimodular on* $C_d \smallsetminus \{0\}$.

The reader should not be confused with the unimodular functions in Enflo's problem that do not vanish at 0 and that are defined in the Appendix.

Problem (H. Cohn) *Let $f : C_d \to \mathbb{C}$ be a unimodular $\mathcal{C}$-function on the cyclic group C_d. Assume $d = p$ is prime. Is the function f proportional to a Dirichlet character?*

Geometric interpretation When the function f is unimodular on $C_d \smallsetminus \{0\}$, Condition (1.1) means that the correlations between f and its translates are constant equal to $\frac{-1}{d-1}$. We will see in Lemma 2.4 that, equivalently, Condition (1.1) means that the Fourier transform $\widehat{f}$ is unimodular on $C_d \smallsetminus \{0\}$.

Before stating our results we gather a few comments. This problem is analogous to the problem of *biunimodular functions* that was raised by Per Enflo in the late 80's and quickly solved by Björck in [9] . See the Appendix for a few words and new results on this analogous problem.

A counterexample to an extension of Cohn's problem, where the finite field $\mathbb{F}_p$ is replaced by a non-prime field $\mathbb{F}_{p^k}$ with $k \geqslant 2$ and $p^k > 4$, was

found by Choi and Siu in 2000 in [13]. Partial positive answers for prime fields were given by Borwein, Choi and Yazdani in 2001 in [11, Cor. 1.2], by Kurlberg in 2002 when the values of f are roots of unity in [24], and by Klurman and Mangerel in 2018 in [23, Section 1.3] who refered to this problem as "Cohn's conjecture".

When $d = p$ is prime, the set of $\mathcal{C}$-functions such that $f(1) = 1$ is finite. This was proven by Biro in 1999 in [7].

1.2 Main results

When d is not prime, no unimodular $\mathcal{C}$-functions on C_d were known to exist. In the following proposition, we remark that they always exist. A function f is said to be odd if $f(-k) = -f(k)$ for all k in C_d.

Proposition 1.1. *Let $d \geqslant 3$ be an odd integer. Then there exist odd unimodular $\mathcal{C}$-functions on the cyclic group C_d.*

The first non trivial case is when $d = 9$. We will see in Section 7.2 that there are exactly 12 odd unimodular $\mathcal{C}$-functions on C_9. All of them are Galois conjugate.

When $d = p$ is prime, Proposition 1.1 is not useful since one already knows that the odd Dirichlet characters are unimodular $\mathcal{C}$-functions. However, in this case, we have a stronger existence result that answers Harvey Cohn's problem.

Theorem 1.2. *Let $p \geqslant 11$ be prime. Then there exist odd unimodular $\mathcal{C}$-functions f on $\mathbb{F}_p$ which are not proportional to a Dirichlet character.*

One can check that, for $p = 3$, 5 and 7, every unimodular $\mathcal{C}$-function on $\mathbb{F}_p$ is proportional to a Dirichlet character.

The first non trivial case of Theorem 1.2 is when $p = 11$. We will see in Section 7.3 that there are exactly 15 odd unimodular $\mathcal{C}$-functions on $\mathbb{F}_{11}$, all of them except one having multiplicity 1. The exception is the Legendre character χ_0. Among these functions there are 5 odd Dirichlet characters. The remaining 10 functions are Galois conjugate.

The functions f on C_d constructed both in Proposition 1.1 and in Theorem 1.2 are more delicate to understand than the Dirichlet characters. Indeed, even when $f(1) = 1$, they may take their values in non-cyclotomic number fields.

Forgetting the unimodularity condition, we will be able to compute the number of odd $\mathcal{C}$-functions f which are normalized, i.e. such that $f(1) = 1$.

Theorem 1.3. *Let p be an odd prime, then, counted with multiplicities, the number of odd $\mathcal{C}$-functions f on $\mathbb{F}_p$ with $f(1) = 1$ is equal to the binomial coefficient $\binom{2k}{k}$ where $k := (p-3)/2$.*

Note that, when $p \equiv 3 \bmod 4$, the multiplicity for the Legendre character $f = \chi_0$ is equal to $2^{(p-1)/2}$. This will be proven in Proposition 5.2.*a*.

1.3 Biunimodular functions

In the appendix, we will apply the same method to a popular analogous problem: the construction of biunimodular functions on $\mathbb{F}_p$. Those are functions of constant modulus whose Fourier transform also has constant modulus. We will construct in Theorem A.1 *new* biunimodular functions on $\mathbb{F}_p$. Here *new* means that the function is neither a gaussian function nor the translate of an $(\mathbb{F}_p^*)^2$-invariant function.

1.4 Organization

Proposition 1.1 will be proven in Chapter 2. Both Proposition 1.1 and Theorem 1.2 will rely on results in symplectic geometry dealing with intersection of a Lagrangian submanifold and its translate by a Hamiltonian diffeomorphism in a compact symplectic manifold. These results, Theorems 2.1 and 2.3, are due to Biran, Entov and Polterovich in [6] and to Cheol-Hyun Cho in [12]. Their proof relies on Floer homology.

Theorem 1.2 will be proven in Chapter 3 for non safe primes p , i.e. when $(p-1)/2$ is non prime. In its proof, it will be crucial to deal with equivariant functions on $\mathbb{F}_p$. This will be useful to check that the known intersections of the corresponding Clifford torus with its image under the Fourier transform are transverse. This transversality will rely on a property of Jacobi sums given in Proposition 3.1.

Proposition 3.1 will be proven in Chapter 4. It will rely on a classical theorem in cyclotomic field theory: the Stickelberger formula for the Jacobi sums.

Theorem 1.2 will be proven in Chapter 5 for safe primes p , i.e. when $(p-1)/2$ is prime. The extra difficulty in this case is that we have to deal with non

transverse tori and to estimate the multiplicity of the intersection at the Legendre character. We will then slightly perturb the Fourier transform so that the known intersections of the tori become transverse.

Theorem 1.3 will be proven in Chapter 6. There we will deal with more general equivariant functions, see Theorem 6.6. In the proof, we adapt a strategy developed by Haagerup in [18] for counting cyclic d-roots. The key ingredient is the little theorem of Chebotarev (Lemma 6.2) as reformulated by Biro and Tao.

A few examples will be given in Chapter 7 that emphasize the complexity of these new $\mathcal{C}$-functions.

Finally we will discuss in the Appendix the adaptation of these methods to the Enflo problem for biunimodular functions.

I would like to thank A. Mangerel who pointed out to me, while I was lecturing on [4] and [5], the Harvey Cohn problem in [27], the Enflo biunimodular vectors problem in [16] and who emphasized the strong analogy between these two problems.

2 Using Symplectic Geometry

In this Chapter we prove Proposition 1.1.

We begin in Section 2.1 by stating a theorem dealing with the unitary group, its action on the complex projective space and the Clifford tori.

We interpret in Section 2.2 the $\mathcal{C}$-functions via the Fourier transform.

We prove in Section 2.3 the existence of unimodular $\mathcal{C}$-functions on C_d.

2.1 The unitary group

We recall that the complex projective space $\mathbb{CP}^{n-1}$ is the set of lines of $\mathbb{C}^n$ that we denote $p = [z_1, \dots, z_n]$. A Clifford torus is a compact $(n-1)$-dimensional torus of the form $\mathbb{T}^{n-1} := \{p = [z_1, \dots, z_n] \in \mathbb{CP}^{n-1} \mid |z_i| = 1 \text{ for all } i\}$ in a unitary basis of $\mathbb{C}^n$. The unitary group $U = U(n)$ acts naturally on $\mathbb{CP}^{n-1}$.

Theorem 2.1. (Biran, Entov, Polterovich, Cho) *Let $\mathbb{CP}^{n-1}$ be the complex projective space and $\mathbb{T}^{n-1} \subset \mathbb{CP}^{n-1}$ be the Clifford torus. Then for all unitary transformation $u \in U$, one has $\mathbb{T}^{n-1} \cap u\mathbb{T}^{n-1} \neq \varnothing$.*

This theorem is due to Biran, Entov and Polterovich in [6] and to Cheol-Hyun Cho in [12]. Both proofs rely on Floer homology. The key remark being that $\mathbb{CP}^{n-1}$ is a closed symplectic manifold, that $\mathbb{T}^{n-1}$ is a closed lagrangian submanifold and that the unitary transformation u is a hamiltonian diffeomorphism of $\mathbb{CP}^{n-1}$. These four authors consider a closed Lagrangian submanifold L in a closed symplectic manifold. Under some extra assumption on L, for instance when L is "monotone", they prove that L cannot be displaced from itself by a hamiltonian diffeomorphism. Therefore, the Clifford torus $\mathbb{T}^{n-1}$ in the projective space $\mathbb{CP}^{n-1}$ cannot be displaced from itself by a unitary operator u in $U(n)$.

Idel and Wolf reformulated in [20] Theorem 2.1 as a decomposition theorem for the unitary group $U = U(n)$.

Let $p_0 = \mathbb{C}v_0$ be the point on the Clifford torus $\mathbb{T}^{n-1}$ where v_0 is the vector $v_0 = (1, \dots, 1)$. Let V be the stabilizer $V := \{u \in U \mid u(v_0) = v_0\}$, and let $T \subset U$ be the maximal torus subgroup $D := \{\mathrm{diag}(u_1, \dots, u_n) \in U\}$.

Corollary 2.2. (Idel, Wolf) *One has the equality $U = DVD$.*

This means that every unitary matrix u can be decomposed as a product of three unitary matrices $u = d_1 v d_2$ with both d_i diagonal and with $\sum_j v_{ij} = 1$ for all $i = 1, \dots, n$. Note that this decomposition is not *unique modulo the center of U*. See [2] for some examples.

The following theorem in [12] is more precise. We recall that an intersection point $p \in \mathbb{T}^{n-1} \cap u\mathbb{T}^{n-1}$ is transverse if the tangent spaces at p intersect transversally, that is if $T_p\mathbb{T}^{n-1} \cap T_p\, u\mathbb{T}^{n-1} = \{0\}$.

Theorem 2.3. (Cho) *Let $\mathbb{CP}^{n-1}$ be the complex projective space of $\mathbb{C}^n$, let $\mathbb{T}^{n-1} \subset \mathbb{CP}^{n-1}$ be the Clifford torus, and $u \in U(n)$ a unitary transformation. If the intersection $\mathbb{T}^{n-1} \cap u\mathbb{T}^{n-1}$ is transverse, it contains at least 2^{n-1} points.*

2.2 The finite Fourier transform

The Harvey Cohn problem can be formulated in terms of Fourier transforms.

In the present paper we focus on the cyclic group $C_d := \mathbb{Z}/d\mathbb{Z}$ where d is an odd integer, which will often be assumed to be prime $d = p$. We will use

the Fourier transform $f \mapsto Ff = \widehat{f}$ on $\mathbb{C}^{C_d}$, with the sign convention given by, for all $k \in C_d$,

$$\widehat{f}(k) = \tfrac{1}{\sqrt{d}} \sum_{\ell \in C_d} e^{2i\pi k\ell/d}\, f(\ell). \tag{2.1}$$

See for instance [33].

A function $f : C_d \to \mathbb{C}$ is said to be *biunimodular* on $C_d \setminus \{0\}$ if both f and $\widehat{f}$ vanish at 0 and are unimodular on $C_d \setminus \{0\}$ as defined in Section 1.1.

The following lemma is a straightforward remark that gives a clean interpretation of the $\mathcal{C}$-functions in term of the Fourier transform.

Lemma 2.4. *a) A function $f : C_d \to \mathbb{C}$ vanishing at 0 is a $\mathcal{C}$-function if and only if there exists a function $g : C_d \to \mathbb{C}$ vanishing at 0 such that*

$$fg = \mathbf{1}_{C_d \setminus \{0\}} \text{ and } \widehat{f}\,\widehat{\breve{g}} = \mathbf{1}_{C_d \setminus \{0\}}. \tag{2.2}$$

b) In particular, a function $f : C_d \to \mathbb{C}$ is a unimodular $\mathcal{C}$-function if and only if f is biunimodular on $C_d \setminus \{0\}$.

Here $\breve{g}$ is the function given by $\breve{g}(x) = g(-x)$. Note that $\widehat{\breve{g}} = \breve{\widehat{g}}$.

Proof. *a)* The function $\sqrt{d}\,\widehat{f}\,\widehat{\breve{g}}$ is the Fourier transform of the convolution $f * \breve{g}$ and the function $\sqrt{d}\,\mathbf{1}_{C_d \setminus \{0\}}$ is the Fourier transform of $d\delta_0 - \mathbf{1}_{C_d}$.

Therefore, Equation (2.2) is equivalent to

$$fg = \mathbf{1}_{C_d \setminus \{0\}} \text{ and } f * \breve{g} = d\,\delta_0 - \mathbf{1}_{C_d}$$

which is nothing but Condition (1.1).

b) Just apply Point *a)* with the function $g = \overline{f}$. □

When $d = p$ is a prime number, every non trivial Dirichlet character χ on $\mathbb{F}_p$ is a unimodular $\mathcal{C}$-function. Indeed, the Fourier transform $\widehat{\chi}$ is proportional to $\overline{\chi}$. Moreover, when $\chi(-1) = -1$, this function χ is odd.

2.3 Existence of unimodular $\mathcal{C}$-functions

Proof of Proposition 1.1. Let $d = 2n + 1$ be an odd integer and V_- be the vector space of odd functions on C_d. By using the basis $(E_j)_{1 \leqslant j \leqslant n}$ of V_- given by $E_j := \delta_j - \delta_{-j}$, one identifies V_- with $\mathbb{C}^n$. The Fourier transform $f \mapsto \widehat{f}$ is a unitary transformation of V_- that we still denote by F. The

elements of the Clifford torus $\mathbb{T}^{n-1}$ of $\mathbb{P}(V_-) = \mathbb{CP}^{n-1}$ are precisely the lines spanned by odd unimodular functions on $C_d \smallsetminus \{0\}$. Theorem 2.1 tells us that $\mathbb{T}^{n-1} \cap F(\mathbb{T}^{n-1}) \neq \varnothing$. By Lemma 2.4.$a$ this exactly means that there exists a unimodular odd $\mathcal{C}$-function. □

3 Equivariant unimodular $\mathcal{C}$-functions

In this Chapter we begin the proof of Theorem 1.2, relying on Proposition 3.1 that will be proven in Chapter 4.

We introduce in Section 3.2 the space of (H, c)-equivariant functions.

We give a criterion in Section 3.3 for the transversality of a Clifford torus and its image by Fourier transform at the points given by Dirichlet characters.

We explain in Section 3.4 the examples where this transversality is not satisfied, and, by avoiding them we deduce the existence of new unimodular $\mathcal{C}$-functions when the prime p is a safe prime.

3.1 The Jacobi sums

Let $p \geqslant 3$ be a prime number. We recall that a Dirichlet character χ on $\mathbb{F}_p$ is said to be *principal* or *trivial* if $\chi \equiv \mathbf{1}$ on $\mathbb{F}_p^*$, and that the order of χ is the smallest positive integer d_χ such that χ^{d_χ} is trivial. The Dirichlet character χ_0 of order 2 is called the Legendre character, since it is given by the Legendre symbol.

In this paper we will always denote by χ_0 the Legendre character. This should not lead to confusion with the standard notation for the principal Dirichlet character. Indeed since the principal Dirichlet character does not satisfy Condition (1.1), it will not play a role in this article.

Let χ_1, χ_2 be two Dirichlet characters. The corresponding Jacobi sum is defined as

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_p} \chi_1(x)\, \chi_2(1-x). \tag{3.1}$$

These algebraic numbers live in the cyclotomic field $K = \mathbb{Q}(\zeta_{p-1})$ spanned by the $(p-1)^{\text{th}}$-root of unity $\zeta_{p-1} = e^{\frac{2i\pi}{p-1}}$

Recall that, one has the equalities

$$J(\chi_1, \chi_2) = J(\chi_2, \chi_1) = \chi_2(-1) J(\overline{\chi}_1 \overline{\chi}_2, \chi_2)$$

When $\chi_1\chi_2$ is not principal, one has the equality

$$J(\chi_1,\chi_2) = \tfrac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}. \tag{3.2}$$

where $G(\chi)$ is the Gauss sum

$$G(\chi) = \sum_{x\in\mathbb{F}_p} \chi(x)\zeta_p^x. \tag{3.3}$$

Therefore, when χ_1, χ_2 and $\chi_1\chi_2$ are not principal, one has

$$|J(\chi_1,\chi_2)| = \sqrt{p}. \tag{3.4}$$

These quantities are useful: the Jacobi sum occurs in the convolution product

$$\chi_1 * \chi_2 \;=\; J(\chi_1,\chi_2)\,\chi_1\chi_2,$$

and, for χ non trivial, the Gauss sum occurs in the Fourier transform

$$\widehat{\chi} = \tfrac{G(\chi)}{\sqrt{p}}\,\overline{\chi}. \tag{3.5}$$

When the Dirichlet character χ is the trivial character $\chi = \mathbf{1}_{\mathbb{F}_p^*}$, one has an extra term: $\widehat{\mathbf{1}_{\mathbb{F}_p^*}} = \frac{-1}{\sqrt{p}}\,\mathbf{1}_{\mathbb{F}_p^*} + \frac{p-1}{\sqrt{p}}\delta_0$.

We will need the following

Proposition 3.1. *Let $p \geqslant 3$ be a prime number and χ_1, χ_2 be two non principal Dirichlet characters. Then one has the equivalence:*

$$\textit{the ratio } R(\chi_1,\chi_2) := \frac{J(\overline{\chi}_1,\chi_2)}{J(\chi_1,\chi_2)} \textit{ is a root of unity} \tag{3.6}$$

if and only if one of the following seven cases is satisfied:
(a) χ_1 has order 2.
(b) $p \equiv 1 \bmod 6$, χ_1 has order 3 and χ_2 has order 6.
(c) $p \equiv 1 \bmod 10$, $\chi_1 = \chi_2^2$ or $\overline{\chi}_2^2$ and χ_2 has order 10.
(d) $p \equiv 1 \bmod 12$, χ_1 has order 4 and χ_2 has order 6.
(e) $p \equiv 1 \bmod 12$, χ_1 has order 3 and χ_2 has order 4.
(f) $p \equiv 1 \bmod 30$, χ_1 has order 5 and χ_2 has order 6.
(g) $p \equiv 1 \bmod 30$, χ_1 has order 3 and χ_2 has order 10.

Proposition 3.1 is an output of Stickelberger's theorem which gives the prime factorization in $\mathbb{Z}[\zeta_{p-1}]$ of the Jacobi sums. We will give a detailed proof in Chapter 4.

We will see in Proposition 3.2 that the meaningful case is when the ratio (3.6) is equal to $\chi_2(-1)$. We will also see that this special value of the ratio does not play a role in the proof and that it can occur in each of these seven cases.

3.2 Equivariant $\mathcal{C}$-functions

Before going on let us explain why we need to deal with equivariant functions. We want to use Theorem 2.3 to prove the existence of $\mathcal{C}$-functions. The Fourier transform F is a unitary operator on the space $\mathbb{C}^{\mathbb{F}_p}$ of functions f on $\mathbb{F}_p$, but it does not preserve the subspace of functions vanishing at 0. We would like to find a vector subspace V of this subspace such that both V and $F(V)$ have a unitary basis for which the sup norm is proportional to the sup norm on $\mathbb{C}^{\mathbb{F}_p}$. The space $V_{H,c}$ of equivariant functions on $\mathbb{F}_p$ will play this role.

Let $p \geqslant 3$ be a prime number, let $C_p = \mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ be the cyclic additive group, and let $G := \mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ be the cyclic multiplicative group. Let $H \subsetneq G$ be a proper subgroup of index $n \geqslant 2$, and $c : H \to \mathbb{C}^*$ be a non-trivial character. We introduce the vector space $V = V_{H,c}$ of (H, c)-equivariant functions f on $\mathbb{F}_p$.

$$V_{H,c} := \{f : \mathbb{F}_p \to \mathbb{C} \mid f(hx) = c(h)f(x) \text{ for all } h \in H,\ x \in \mathbb{F}_p\}. \tag{3.7}$$

Note that all (H, c)-equivariant functions f vanish at 0: one has $f(0) = 0$. We denote by $g_1 = 1, g_2, \ldots, g_n$ a family of representatives in G of the classes gH, and by $(f_i)_{1 \leqslant i \leqslant n}$ the family of elements of V defined by $f_i(g_j) = \delta_{i,j}$ for all i, j. This family is a basis of V. More precisely any function f in V can be written in a unique way as $f = \sum_{1 \leqslant i \leqslant n} \lambda_i f_i$ with $\lambda_i \in \mathbb{C}$ and one has the equality of the sup norms

$$\sup_{x \in \mathbb{F}_p} |f(x)| = \sup_{1 \leqslant i \leqslant n} |\lambda_i|.$$

3.3 Transversality of Clifford tori

Let $\mathbb{P}(V_{H,c}) \simeq \mathbb{CP}^{n-1}$ be the projective space of $V_{H,c}$ and $T_{H,c}$ be the Clifford torus

$$T_{H,c} := \{[f] \in \mathbb{P}(V_{H,c}) \mid \ |f(x)| = |f(1)| \text{ for all } x \in \mathbb{F}_p^*\} \simeq \mathbb{T}^{n-1}. \tag{3.8}$$

The vector space $V_{H,c}$ contains exactly n Dirichlet characters χ. The points $[\chi]$ belong to $T_{H,c}$. Since the Fourier transform $F : f \mapsto \widehat{f}$ is a unitary transformation that sends $V_{H,c}$ onto $V_{H,\overline{c}}$ where $\overline{c}$ is the conjugate character, we will have to deal with two hermitian vector spaces instead of one. This will not be an issue when applying Cho's theorem. Indeed one can choose a unitary transformation $u_0 : V_{H,\overline{c}} \xrightarrow{\sim} V_{H,c}$ such that $u_0(T_{H,\overline{c}}) = T_{H,c}$ and apply Cho's theorem to the unitary transformation $u := u_0 \circ F$ of $V_{H,c}$.

According to (3.5), the points $[\chi] \in \mathbb{P}(V_{H,c})$ belong to $T_{H,c} \cap F^{-1}T_{H,\overline{c}}$.

Proposition 3.2. *Let χ be a character of $G := \mathbb{F}_p^*$ that extends the non trivial character c of a subgroup $H \subset G$. The intersection $T_{H,c} \cap F^{-1}T_{H,\overline{c}}$ is transverse at $[\chi]$ if and only if, for every non trivial character ψ of G which is trivial on H, one has*

$$J(\chi, \psi) \neq \psi(-1)\, J(\overline{\chi}, \psi). \tag{3.9}$$

We will see in Proposition 3.4 nice conditions on (H, c) that ensure (3.9).

Remark 3.3. Note that the factor $\psi(-1)$ is nothing but a sign which is given by the parity of ψ. When H has even order, the element -1 belongs to H and this sign is equal to $+1$.

Proof of Proposition 3.2. Let $d = p-1$, and write $d = n\, d_H$ where n is the index of H and d_H the order of H.

⋆ **We first describe the tangent space to the projective space.** We fix χ as in the proposition and we set

$$\begin{aligned} B = B_{H,c} &:= \{\chi' \text{ character of } G \mid \chi' \in V_{H,c}\}, \\ B_o := B_{H,o} &:= \{\psi \text{ character of } G \text{ trivial on } H\}. \end{aligned}$$

The set B is a basis of $V_{H,c}$. Similarly, the set B_o is a basis of the space $V_{H,o}$ of H-invariant functions on $\mathbb{F}_p$ that vanish at 0. Moreover every element χ'

of B can be written in a unique way as $\chi' = \chi\psi$ with ψ in B_o. This basis B is orthogonal: one has, for χ', χ'' in B,

$$\langle \chi', \chi'' \rangle_{\ell^2(\mathbb{F}_p)} = \begin{cases} p-1 & \text{if } \chi' = \chi'' \\ 0 & \text{otherwise.} \end{cases}$$

We set $B'_o := B_o \smallsetminus \{\psi_0\}$ where $\psi_0 = \mathbf{1}_G \in B_o$ is the trivial character of G. It will be convenient to use the following coordinates system $\mathbf{a} = (\mathbf{a}_\psi)_{\psi \in B'_o}$ of $\mathbb{P}(V)$ in the neighborhood of $[\chi]$ where the coordinates $\mathbf{a}_\psi$ are complex numbers. It is given by

$$\mathbf{a} \mapsto [f_{\mathbf{a}}] \;\text{ where }\; f_{\mathbf{a}} = \left(\mathbf{1}_G + \textstyle\sum_{\psi \in B'_o} \mathbf{a}_\psi \psi\right) \chi \,. \tag{3.10}$$

These coordinates $\mathbf{a} = (\mathbf{a}_\psi) \in \mathbb{C}^{B'_o}$ are also a linear coordinate system for the tangent space of $\mathbb{P}(V)$ at the point $[\chi]$, thanks to the formula

$$\mathbf{a} \mapsto v_{\mathbf{a}} := \frac{d}{d\varepsilon}[f_{\varepsilon \mathbf{a}}]|_{\varepsilon=0} \;\in\; T_{[\chi]}\mathbb{P}(V_{H,c}).$$

⋆ **We describe the tangent space to the Clifford torus** $T_{H,c}$. The real linear equations defining the tangent space of $T_{H,c}$ at the point $[\chi]$ are

$$\frac{d}{d\varepsilon}\left(|f_{\varepsilon\mathbf{a}}(x)|^2 - |f_{\varepsilon\mathbf{a}}(1)|^2\right)\big|_{\varepsilon=0} \;=\; 0\,, \quad \text{for all } x \text{ in } G.$$

Since $\psi(1) = 1$ for all ψ in B_o, using (3.10), this can be rewritten as

$$\mathrm{Re}(\textstyle\sum_{\psi \in B'_0} \mathbf{a}_\psi(\psi - \psi_0)) \;=\; 0. \tag{3.11}$$

Since the basis B_o is invariant by complex conjugation, Condition (3.11) can be rewritten as

$$\textstyle\sum_{\psi \in B'_0} (\overline{\mathbf{a}_{\overline{\psi}}} + \mathbf{a}_\psi)\,(\psi - \psi_0) \;=\; 0.$$

By the linear independance of the characters of G/H, this gives

$$T_{[\chi]}T_{H,c} \;\simeq\; \{(\mathbf{a}_\psi) \in \mathbb{C}^{B'_o} \mid \overline{\mathbf{a}_{\overline{\psi}}} = -\mathbf{a}_\psi \;\text{ for all } \psi \in B'_o\}. \tag{3.12}$$

⋆ **We describe the tangent space to the torus** $F^{-1}T_{H,\bar{c}}$. Using (3.5), one computes in our coordinate system

$$\widehat{f_{\mathbf{a}}} = \tfrac{G(\chi)}{\sqrt{p}} \left(\mathbf{1}_G + \textstyle\sum_{\psi \in B'_o} \alpha_\psi \mathbf{a}_\psi \overline{\psi}\right) \overline{\chi}$$

where we have, using also (3.2),

$$\alpha_\psi \ := \ \frac{G(\chi\psi)}{G(\chi)} \ = \ \frac{G(\psi)}{J(\chi,\psi)} \ . \tag{3.13}$$

One deduces from (3.12) the equality

$$T_{[\chi]}F^{-1}T_{H,\bar{c}} \ \simeq \ \{(\mathbf{a}_\psi) \in \mathbb{C}^{B'_o} \mid \overline{\alpha_{\overline{\psi}}}\,\overline{\mathbf{a}_{\overline{\psi}}} = -\alpha_\psi\,\mathbf{a}_\psi \text{ for all } \psi \in B'_o\}. \tag{3.14}$$

$\star$ **We give the transversality criterion for the tangent spaces**. One easily computes

$$\overline{\alpha_{\overline{\psi}}} \ = \ \frac{\overline{G(\overline{\psi})}}{\overline{J(\chi,\overline{\psi})}} \ = \ \frac{\psi(-1)\,G(\psi)}{J(\overline{\chi},\psi)} \ . \tag{3.15}$$

Comparing (3.12) and (3.14), and using the values (3.13) and (3.15) for α_ψ and $\overline{\alpha_{\overline{\psi}}}$, one gets the equivalences:

$$\begin{aligned} T_{[\chi]}T_{H,c} \cap T_{[\chi]}F^{-1}T_{H,\bar{c}} = \{0\} \ &\iff \ \overline{\alpha_{\overline{\psi}}} \neq \alpha_\psi \ \text{ for all } \psi \in B'_o \\ &\iff \ J(\chi,\psi) \neq \psi(-1)\,J(\overline{\chi},\psi) \ \text{ for all } \psi \in B'_o. \end{aligned}$$

This ends the proof of Proposition 3.2. □

3.4 Unimodular $\mathcal{C}$-functions for non safe prime

In this section we explain how to check that the intersection $T_{H,c} \cap F^{-1}T_{H,\bar{c}}$ is not transverse at a Dirichlet character $[\chi]$. We deduce from that the existence of new unimodular $\mathcal{C}$-functions for a non safe prime p.

Let $p \geqslant 3$ be prime. Let $H \subsetneq \mathbb{F}_p^*$ be a proper subgroup of index n and $c : H \to \mathbb{C}^*$ be a non-trivial character of order d_c. Let $V = V_{H,c}$ be the n-dimensional vector space of (H,c)-equivariant functions f on $\mathbb{F}_p$ as in (3.7).

Proposition 3.4. *Assume that we are not in one of the four cases*
(i) $d_c = 2$ *and* n *is odd,*
(ii) $d_c = 2$ *and* $n \equiv 6$ *mod* 12*,*
(iii) $d_c = 3$ *and* n *is a multiple of* 4 *or* 10 *and* n *is coprime to* 3*,*
(iv) $d_c = 5$ *and* n *is a multiple of* 6 *and* n *is coprime to* 5*.*

a) Then the intersection $T_{H,c} \cap F^{-1}T_{H,\bar{c}}$ is transverse at $[\chi]$, for all Dirichlet character χ extending c.
b) When $n \geqslant 3$, there exists in $V_{H,c}$ a unimodular $\mathcal{C}$-function which is not proportional to a Dirichlet character.

Here is a comment on Case (i), and more precisely when the order of χ is 2. Recall that there is only one Dirichlet character χ_0 of order 2. It is given by the Legendre symbol: $\chi_0(x) = (\frac{x}{p})$ for all x in $\mathbb{F}_p$. It belongs to $V_{H,c}$ if and only if $d_c = 2$ and n is odd. In this case, the intersection $T_{H,c} \cap F^{-1}T_{H,\bar{c}}$ is not transverse at $[\chi_0]$. In this case it will be more delicate to apply Theorem 2.3. This will be done in Chapter 5.

Proof of Proposition 3.4. a) This follows from Propositions 3.1 and 3.2. We look at the lists of exceptions (d_χ, d_ψ) in Proposition 3.1 remembering that d_χ is a multiple of d_c and that d_ψ divides n. We also use the fact that, when the index n is not coprime to d_c, the character c of H does not admit an extension χ of order d_c. In particular, using the labeling of Proposition 3.1, Case (a) implies (i), Case (b) cannot occur, Case (c) also cannot occur, Case (d) implies (ii). Case (e) implies (iii), Case (f) implies (iv) and Case (g) also implies (iii).

b) Assume, by contradiction that the intersection $T_{H,c} \cap F^{-1}T_{H,\bar{c}}$ contains only Dirichlet characters $[\chi]$. Then, by Point *a)*, this intersection is transverse. Therefore Theorem 2.3 predicts the existence of at least 2^{n-1} intersection points. Since $n \geqslant 3$, one has $2^{n-1} > n$. Since the number of Dirichlet characters in $V_{H,c}$ is n, there must exist another intersection point. This is the contradiction we are looking for. □

A prime p for which $(p-1)/2$ is prime is called a safe prime. For instance $p = 7$, 11, 23, 47, ... Most of the primes are non safe, see [19, Thm 3.12]. But, conjecturally, there are infinitely many safe primes.

Corollary 3.5. *Let $p \geqslant 11$ be a non safe prime.*
a) There exist a subgroup $H \subset \mathbb{F}_p^*$ of index $n \geqslant 3$ containing -1 and an odd character c of H such that, for all Dirichlet character χ in $V_{H,c}$, the intersection $T_{H,c} \cap F^{-1}T_{H,\bar{c}}$ is transverse at $[\chi]$.
b) For such a pair (H, c) the space $V_{H,c}$ contains an odd unimodular $\mathcal{C}$-function f which is not proportional to a Dirichlet character.

Proof of Corollary 3.5. *a*) We recall that an odd character c of H is a character such that $c(-1) = -1$. For such a character, all the functions f in $V_{H,c}$ are odd. We set $d = p-1$ and distinguish two cases.

First case: d has an odd prime factor ℓ.
We set $r := d/\ell$. We choose H to be the subgroup of $\mathbb{F}_p^*$ of prime index $n := \ell \geqslant 3$ and c to be a character of H of order $d_c := r \geqslant 3$. Since these values do not occur in the exceptions of Proposition 3.4 the intersection $T_{H,c} \cap F^{-1}T_{H,\bar{c}}$ is transverse at $[\chi]$. This group H contains -1 and one has $c(-1) = -1$.

Second case: d is a power of 2.
We set $r := d/4$. It is also a power of 2. We choose H to be the subgroup of $\mathbb{F}_p^*$ of index $n := 4$ and c to be the character of H of order $d_c := r$.

Again, since these values do not occur in the exceptions of Proposition 3.4 the intersection $T_{H,c} \cap F^{-1}T_{H,\bar{c}}$ is transverse at $[\chi]$. This group H contains -1 and one has $c(-1) = -1$.

b) By the proof of Proposition 3.4, the space $V_{H,c}$ contains a unimodular $\mathcal{C}$-function f on $\mathbb{F}_p^*$ which is not proportional to a Dirichlet character. □

Remark 3.6. The conclusion of Proposition 3.4.*a*, i.e. the transversality of the intersection, is not true in the exceptional cases $(i) - (iv)$ for infinitely many values of p.

Remark 3.7. There also exist even counterexamples to Harvey Cohn's question for all primes $p \geqslant 5$ for which $\frac{p-1}{2}$ is not of the form q, $2q$, $3q$ or $5q$ with q prime.

Indeed, applying Proposition 3.4.b) with a subgroup $H \subset \mathbb{F}_p^*$ of index $n \geqslant 3$ containing -1 and with an even character c of H of order d_c satisfying none of the four conditions $(i), \ldots, (iv)$, one gets an even unimodular $\mathcal{C}$-function which is not proportional to a Dirichlet character.

However, the existence of an even counterexample to Cohn's question for all sufficiently large prime p is still an open question.

4 Using cyclotomic field theory

The aim of this Chapter is to prove Proposition 3.1. I give a full proof since I did not find a reference for it. The key ingredient is the Kummer-Stickelberger formula which is a formula that give, both for Gauss sums and for Jacobi sums, an explicit factorization as a product of prime ideals.

In Section 4.1, we begin by a combinatorial lemma which parametrizes the orbits of $(\mathbb{Z}/d\mathbb{Z})^*$ acting on $(\mathbb{Z}/d\mathbb{Z})^2$. The proof involves many cases.

In Section 4.2 we recall the short and elementary calculation which implies the Stickelberger's theorem.

In Section 4.3, we use this combinatorial lemma together with the Stickelberger theorem to distinguish various Jacobi sums.

In Section 4.4, we point out surprising equalities between Jacobi sums that prevent the corresponding Clifford tori to intersect transversally.

4.1 Action on $(\mathbb{Z}/d\mathbb{Z})^2$

We will need the following combinatorial lemma. Let $d \geqslant 2$ be an integer. We introduce an equivalence relation $(j,k) \sim (j',k')$ on $\mathbb{Z}^2$ given by

$$\begin{array}{c} \text{there exists an integer } x \text{ coprime to } d \text{ such that} \\ j' = xj \bmod d \quad \text{and} \quad k' = xk \bmod d. \end{array} \tag{4.1}$$

We will see that these equivalence classes are related to the orbits of the Galois group acting on the Jacobi sums. The following lemma gives a nice representative in each equivalence class.

Lemma 4.1. *Let $d \geqslant 2$ be an integer. For every positive integers $j,k < d$, there exist positive integers $j',k' < d$ such that*

$$\begin{array}{l} (j',k') \sim (j,k) \ \text{ or } \ (j',k') \sim (-j,k)\,, \\ \text{and} \quad\ j' \leqslant k' \leqslant d - j', \end{array} \tag{4.2}$$

except in one of the following seven cases, where $m \geqslant 1$ is an integer:
(a) $d = 2\,m,\ \ j = m \ \ and \ \ k \neq m.$
(b) $d = 6\,m,\ \ j \equiv \pm 2\,m \bmod d \ \ and \ \ k \equiv \pm m \bmod d.$
(c) $d = 10\,m,\ j \equiv \pm 2\,k \bmod d \ \ and \ \ k \equiv \pm m \ or \ \pm 3\,m \bmod d.$
(d) $d = 12\,m,\ j \equiv \pm 3\,m \bmod d \ \ and \ \ k \equiv \pm 2\,m \bmod d.$
(e) $d = 12\,m,\ j \equiv \pm 4\,m \bmod d \ \ and \ \ k \equiv \pm 3\,m \bmod d.$
(f) $d = 30\,m,\ j \equiv \pm 6\,m \ or \ \pm 12\,m \bmod d \quad and \quad k \equiv \pm 5\,m \bmod d.$
(g) $d = 30\,m,\ j \equiv \pm 10\,m \quad and \quad k \equiv \pm 3\,m \ \ or \ \pm 9\,m \bmod d.$

Remark 4.2. Note that in each of these seven cases (a) to (g), one can not find a pair (j',k') satisfying (4.2).

For the proof we will need the Jacobsthal function $g(n)$ which is the largest gap in the sequence of integers coprime to n. Among $g(n)$ consecutive integers, there is always one which is coprime to n. This gap $g(n)$ grows very slowly with n. It can be bounded by a function that depend only on the number $\omega(n)$ of prime factors of n. Here, we will only need an upper bound on $g(n)$ which is due to Kanold.

Lemma 4.3. ([22]) *For all integers $n \geqslant 2$, one has $g(n) \leqslant 2^{\omega(n)}$.*
In particular one has $g(n) \leqslant n/3$ as soon as $n > 10$.

Proof of Lemma 4.1. We assume that $j, k < d$ are positive integers for which one can not find integers j', k' satisfying (4.2), and we want to prove that we are in one of the seven cases $(a), \ldots, (g)$.

First step: We can assume that $d = jr$ with r integer $r \geqslant 3$.
Indeed there exists an integer x coprime to d such that $xj = j' \bmod d$ and j' is a positive divisor of d so that $d = j'r$ with $r \geqslant 2$. If $r = 2$, this is Case (a).

Second step: We can assume that j is coprime to k.
Indeed if this is not the case we argue by induction. We introduce the integer $m := \gcd(j, k)$ and set $j_0 := j/m$, $k_0 := k/m$ and $d_0 := d/m$. We find an equivalent pair (j'_0, k'_0) satisfying (4.2) with the integer d_0. Then the pair $(j', k') := (mj'_0, mk'_0)$ satisfies (4.2) with the integer d.

Third step: We can assume that $k < j$.
Indeed since (4.2) is not satisfied we have either $k < j$ or $k > d - j$. In the second case, we replace the pair (j, k) by $(j', k') := (j, d - k) \sim (-j, k)$.

Fourth step: We can assume that j is coprime to r.
Indeed let $s := gcd(r, j)$ and $t := lcm(r, j) = d/s$. Assume by contradiction that $s \geqslant 2$. The subset

$$\begin{aligned} S &:= \{x \in \mathbb{Z}/d\mathbb{Z} \mid x \equiv 1 \bmod t\} \\ &= \{1, 1+t, 1+2t, \ldots, 1+(s-1)t\} \end{aligned}$$

is a subgroup of $(\mathbb{Z}/d\mathbb{Z})^*$ of order s, and one has $xj \equiv j \bmod d$, for all x in S. Since, by the second step, k is coprime to s, the cardinality of the set Sk is also equal to s and one has

$$Sk := \{k' \in \mathbb{Z}/d\mathbb{Z} \mid k' \equiv k \bmod t\}.$$

When $r \geqslant 4$, since one has $s \geqslant 2$, the set Sk contains an element k' with $j \leqslant k' \leqslant d - j$.

When $r = 3$, one has $s = 3$ and the set Sk still contains an element k' with $j \leqslant k' \leqslant d - j$.

Fifth step: When $j = 2$, one has $3\,g(d) \geqslant d+2$.
In this case, one has $k = 1$. We remark that the interval $I := [d/3, 2d/3]$ does not contain integers coprime to j. Indeed, when an integer x is in this interval, the integers $j' := |2x-d|$ and $k' := x$ satisfy (4.2), i.e. one has the two inequalities

$$j' \leqslant k' \leqslant d - j'.$$

Therefore the integers x in the interval I are never coprime to j. Since the number of integers in this interval I is at least $(d-1)/3$, this proves the lower bound for the Jacobsthal function

$$g(d) \geqslant (d+2)/3. \tag{4.3}$$

Sixth step: One always has $r\,g(j) \geqslant (r-2)j+2$.
In this step, we will use again the fact that one can not find an integer x coprime to d for which the corresponding pair (j', k') satisfies (4.2). We will only focus on the subgroup of $(\mathbb{Z}/d\mathbb{Z})^*$

$$S := \{x \in (\mathbb{Z}/d\mathbb{Z})^* \mid x \equiv 1 \bmod r\}.$$

Note that, for all x in S, the integer $j' := j$ satisfies $j' \equiv xj \bmod d$. Since k and r are both coprime to j, one can find integers ℓ and s such that

$$\ell k \equiv sr \equiv 1 \bmod j.$$

We will check that the interval $I := \left[sk + \dfrac{j-k}{r}, sk + \dfrac{d-j-k}{r}\right]$ does not contain integers coprime to j. Indeed, when an integer $y = sk + m$ is in this interval and is coprime to j, the element

$$x := 1 + m\ell r \;\equiv\; \ell r y \mod j$$

is also coprime to j, hence it belongs to S. Moreover the element

$$k' := k + (y - sk)r \;=\; k + mr \;\equiv\; xk \bmod d$$

satisfies

$$j' \leqslant k' \leqslant d - j'.$$

Therefore the integers y in the interval I are never coprime to j.

Since the number of integers in this interval I is at least $(r-2)(j-1)/r$, this proves the lower bound for the Jacobsthal function

$$g(j) \geqslant ((r-2)j+2)/r. \tag{4.4}$$

Seventh step: We list the possible values of j and r.
We first notice that since $r \geqslant 3$, Inequality (4.4) tells us that $g(j) > j/3$. Lemma 4.3 tells us then that $j \leqslant 10$. We then distinguish according to the values of j.

⋆ **When $j = 2$.** Inequality (4.3) tells us that $g(d) > d/3$. Lemma 4.3 tells us then that $d \leqslant 10$. Since r is coprime to j. This gives $r = 3$ or $r = 5$.

⋆ **When $j = 3, 4, 5, 7, 8$ or 9.** In these cases one has $g(j) = 2$. Inequality (4.4) tells us that $(j-2)r \leqslant 2j-2$. Since $r \geqslant 3$, this implies that $j \leqslant 4$. Since r is coprime to j, for $j = 3$ this gives $r = 4$, and for $j = 4$ this gives $r = 3$.

⋆ **When $j = 6$ or 10.** In these cases one has $g(j) = 4$. Inequality (4.4) tells us that $(j-4)r \leqslant 2j-2$. Since r is coprime to j, for $j = 6$ this gives $r = 5$, and for $j = 10$ this gives $r = 3$.

Eigth step: We analyze each of these six subcases.

⋆ **When $j = 2$ and $r = 3$:** One has $d = 6$ and $k = 1$. This is Case (b).

⋆ **When $j = 2$ and $r = 5$:** One has $d = 10$ and $k = 1$. This is Case (c).

⋆ **When $j = 3$ and $r = 4$:** One has $d = 12$ and $k = 1$ or 2. The subcase $k = 1$ is excluded since $(3, 1) \sim (3, 5)$. The subcase $k = 2$ is Case (d).

⋆ **When $j = 4$ and $r = 3$:** One has $d = 12$ and $k = 1$ or 3. The subcase $k = 1$ is excluded since $(4, 1) \sim (4, 7)$. The subcase $k = 3$ is Case (e).

⋆ **When $j = 6$ and $r = 5$:** One has $d = 30$ and $k = 1$ or 5. The subcase $k = 1$ is excluded since $(6, 1) \sim (6, 11)$. The subcase $k = 5$ is Case (f).

⋆ **When $j = 10$ and $r = 3$:** One has $d = 30$ and $k = 1, 3, 7$ or 9.
The cases $k = 1$ or 7 are excluded since $(10, 1) \sim (10, 7) \sim (10, 19)$.
The cases $k = 3$ or 9 are equivalent since $(10, 3) \sim (10, 9)$. This is Case (g). □

4.2 The Stickelberger's formula

We will not use the full strength of Stickelberger's formula that can be found in [25, Chap.1] or in [21, Chap.14]. Instead we will use the following elementary formula that was already known to Kummer and that is one of the key ingredients in its proof.

Lemma 4.4. *Let $\mathbb{F}_p$ be a prime field, let j, k be integers $0 < j, k < p-1$. Let us define the Jacobi sum mod p by* $J_{j,k} := \sum_{x \neq 0,1} x^{-j}(1-x)^{-k} \in \mathbb{F}_p$.

a) One has the equality $J_{j,k} = -\binom{j+k}{k}$ in $\mathbb{F}_p$.
b) In particular, one has the equivalence $J_{j,k} \neq 0 \Longleftrightarrow j + k < p$.

Here the sum is over all x in $\mathbb{F}_p$ with $x \neq 0$, $x \neq 1$ and the right-hand side is the binomial coefficient $\binom{j+k}{k} = \frac{(j+k)!}{j!\,k!}$.

Proof of Lemma 4.4. This is a classical and elementary calculation

$$\begin{aligned} J_{j,k} &= \sum_{x \neq 0} x^{-j}(1-x)^{p-1-k} = \sum_{\ell=0}^{p-1-k} (-1)^{\ell} \tbinom{p-1-k}{\ell} \sum_{x \neq 0} x^{\ell - j} \\ &= -(-1)^{j} \tbinom{p-1-k}{j} = -\tbinom{j+k}{k}, \end{aligned}$$

which is valid since the base field is $\mathbb{F}_p$. □

4.3 Distinguishing Jacobi sums

We can now give the proof of $\Longrightarrow$ in Proposition 3.1.

Notation We will prove Proposition 3.1 by reducing (3.6) modulo a suitable prime ideal $\mathfrak{p}$ of the ring $\mathbb{Z}[\zeta_{p-1}]$. More precisely, the multiplicative group $\mathbb{F}_p^*$ is a cyclic group of order $d := p-1$. We denote by g_0 the smallest positive integer whose image modulo p is a generator of $\mathbb{F}_p^*$ and we denote by ω the Teichmüller character of $\mathbb{F}_p^*$ which is defined by the equality $\omega(g_0) = \zeta_{p-1}$. This character is a generator of the group of characters of $\mathbb{F}_p^*$. In particular, since χ_1 and χ_2 are not principal, there exist positive integers $j, k < p-1$ such that

$$\chi_1 = \omega^{-j}\ ,\ \ \chi_2 = \omega^{-k}\ ,\ \text{and hence}\ \ \overline{\chi}_1 = \omega^{-(p-1-j)}.$$

Proof of the implication $\Longrightarrow$ in Proposition 3.1. We assume that we are not in one of the seven cases $(a)-(g)$. In particular, one has $j \neq \frac{p-1}{2}$. The action of an element of the Galois group of $K/\mathbb{Q}$ commutes with the complex conjugation and hence preserves the assertion (3.6). This action is given by an element $a \in (\mathbb{Z}/d\mathbb{Z})^*$ and sends the characters ω^{-j} and ω^{-k} respectively to the characters ω^{-aj} and ω^{-ak}. Therefore, without loss of generality by using the combinatorial Lemma 4.1, we can assume that

$$j \leqslant k \text{ and } j+k \leqslant p-1.$$

We first deal with the case where $j=k$. In this case, one has $j=k<\frac{p-1}{2}$ and, by (3.4), the Jacobi sums in (3.6) do not have the same absolute value. This proves that the ratio (3.6) is not a root of unity.

We now deal with the case where $j<k$. The Jacobi sum $J(\chi_1,\chi_2)$ lives in the ring of integers $\mathcal{O}_K := \mathbb{Z}[\zeta_{p-1}]$. Since the polynomial $X^{p-1}-1$ has $p-1$ distinct root in $\mathbb{F}_p$, the cyclotomic polynomial $\Phi_{p-1}(X)$ is also split in $\mathbb{F}_p$ and has $\varphi(p-1)$ roots in $\mathbb{F}_p$ where φ is the Euler totient. These roots are the generators of the group $\mathbb{F}_p^*$. We denote by $\mathfrak{p}$ the prime ideal of $\mathcal{O}_K$ over p containing $g_0-\zeta_{p-1}$. We denote by

$$\pi_{\mathfrak{p}} : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$$

the natural morphism given by the reduction modulo $\mathfrak{p}$ so that one has $\pi_{\mathfrak{p}}(\omega(x)) = x$ for all x in $\mathbb{F}_p$. Using the notation and the result of Lemma 4.4, one has the equalities

$$\pi_{\mathfrak{p}}(J(\chi_1,\chi_2)) = \pi_{\mathfrak{p}}(J(\omega^{-j},\omega^{-k})) = J_{j,k} = \tbinom{j+k}{k} \neq 0$$

since $j+k \leqslant p-1$. Similarly, one has the equalities

$$\pi_{\mathfrak{p}}(J(\overline{\chi}_1,\chi_2)) = \pi_{\mathfrak{p}}(J(\omega^{-(p-1-j)},\omega^{-k})) = J_{p-1-j,k} = \tbinom{p-1-j+k}{k} = 0$$

since $j<k$. This proves that the ratio (3.6) is not a root of unity. □

4.4 Example of equalities between Jacobi sums

In this section we give the proof of $\Longleftarrow$ in Proposition 3.1. We also explain that the ratios (3.6) are frequently equal to 1 in each of the seven cases.

Proof of $\Longleftarrow$ *in Proposition 3.1.* We want to prove that in each of the seven cases of Proposition 3.1, the ratio $R(\chi_1, \chi_2)$ in (3.6) is a $(p-1)^{\text{th}}$-root of unity.

This ratio is the ratio of two algebraic integers in the cyclotomic field $K = \mathbb{Q}[\zeta_{p-1}]$ all of whose conjugate have the same absolute value equal to $\sqrt{p}$. The pairs $(\chi_1, \chi_2) = (\omega^{-j}, \omega^{-k})$, in these seven cases are exactly those for which one can not find a pair (j', k') satisfying (4.2). By Stickelberger's formula,this means that the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ over p that contain $J(\chi_1, \chi_2)$ is exactly the same as the set of prime ideals of $\mathcal{O}_K$ over p that contain $J(\overline{\chi}_1, \chi_2)$. Since $J(\chi_1, \chi_2)$ has absolute value $\sqrt{p}$, and since the ideal (p) of $\mathcal{O}_K$ is a product of distinct prime ideals, the ratio $R(\chi_1, \chi_2)$ is a unit in K. Since all the Galois conjugates of this ratio $R(\chi_1, \chi_2)$ have absolute value equal to 1, this ratio is a root of unity in $K = \mathbb{Q}[\zeta_{p-1}]$, hence it is a $(p-1)^{\text{th}}$-root of unity. □

Remark 4.5. One can also check the following facts that we will not use.
In Cases (a) and (e), the ratio $R(\chi_1, \chi_2)$ is always equal to 1.
In Case (b) and (g), the ratio $R(\chi_1, \chi_2)$ is always a cubic root of unity.
In Cases (c) and (f), the ratio $R(\chi_1, \chi_2)$ is always a fifth root of unity.
In Case (d), the ratio $R(\chi_1, \chi_2)$ is always equal to ± 1.

Examples: In these seven cases, one does not always have the equality $R(\chi_1, \chi_2) = \chi_2(-1)$. This depends on the prime p and on the parity of χ_2. But in each of these seven cases, there are many primes p for which

$$R(\chi_1, \chi_2) = \chi_2(-1) = 1. \tag{4.5}$$

One can compute the smallest value of p for which (4.5) holds:
In Case (a): $p = 7$. One has $J(\omega^3, \omega^2) = J(\omega^{-3}, \omega^2) = 2 - i\sqrt{3}$.
In Case (b): $p = 109$. One has $J(\omega^{36}, \omega^{18}) = J(\omega^{-36}, \omega^{18}) = -1 - 6i\sqrt{3}$.
In Case (c): $p = 241$. One has $J(\omega^{48}, \omega^{24}) = J(\omega^{-48}, \omega^{24})$.
In Case (d): $p = 37$. One has $J(\omega^9, \omega^6) = J(\omega^{-9}, \omega^6) = -5 + 2i\sqrt{3}$.
In Case (e): $p = 73$. One has $J(\omega^{24}, \omega^{18}) = J(\omega^{-24}, \omega^{18}) = 8 + 3i$.
In Case (f): $p = 601$. One has $J(\omega^{120}, \omega^{100}) = J(\omega^{-120}, \omega^{100}) = \frac{23 - 25i\sqrt{3}}{2}$.
In Case (g): $p = 421$. One has $J(\omega^{140}, \omega^{42}) = J(\omega^{-140}, \omega^{42})$.

Remark 4.6. In these seven cases, when $R(\chi_1, \chi_2) = 1$ and χ_2 is even, one can also check the following facts that we will not use.
In Case (a), $J(\chi_1, \chi_2)$ belongs to $\mathbb{Z}[e^{2i\pi/(p-1)}]$.
In Cases (b), (d) and (f), $J(\chi_1, \chi_2)$ belongs to $\mathbb{Z}[e^{2i\pi/3}]$.

In Case (c) and (g), $J(\chi_1, \chi_2)$ belongs to $\mathbb{Z}[e^{2i\pi/5}]$.
In Case (e), $J(\chi_1, \chi_2)$ belongs to $\mathbb{Z}[e^{2i\pi/4}]$.

This ends the proof of Proposition 3.1 and hence this also ends the proof of Theorem 1.2 for non safe primes.

5 Unimodular $\mathcal{C}$-functions for safe primes

The aim of this chapter is to prove Theorem 1.2 when the prime p is safe, i.e. when the integer $n := (p-1)/2$ is prime. We will work with the projective space $\mathbb{P}(V)$ of the space V of odd functions on $\mathbb{F}_p$, its Clifford torus T and the Fourier transform F. The new difficulty in this case is that the Clifford tori T and $F^{-1}T$ are not transverse at the intersection point $[\chi_0]$ given by the Legendre character χ_0. Indeed they are tangent at that point.

To overcome this difficulty, we will study the "Hessian" of this intersection and prove that it is anisotropic in Lemmas 5.3 and 5.9. This will prove that the algebraic multiplicity at $[\chi_0]$ of the intersection $T \cap F^{-1}T$ is equal to 2^{n-1}, see Proposition 5.2.a.

At first glance, since this number 2^{n-1} is the one predicted by Theorem 2.3, this information seems useless. To go on we will find a small unitary perturbation F_t of the Fourier transform F so that, in a neighborhood of $[\chi_0]$ the intersection $T \cap F_t^{-1}T$ is transverse and contains at most 2^{n-2} points, see Proposition 5.2.b. This will allow us to conclude.

5.1 Strategy

In this section we explain in more detail the strategy and prove Theorem 1.2 for safe primes, taking for granted Proposition 5.2 that will be proven later in this chapter. We will keep the following notation for most of Chapter 5.

Let $p \geqslant 7$ be a safe prime. Let $H_0 = \{\pm 1\} \subset \mathbb{F}_p^*$ and let c_0 be the non trivial character of H_0. Let

$$V = V_{H_0,c_0} = \{f : \mathbb{F}_p \to \mathbb{C} \mid \ f \text{ is odd}\},$$

$$T = T_{H_0,c_0} = \{[f] \in \mathbb{P}(V) \mid \ |f| \text{ is constant}\}.$$

Let $F : V \to V$ be the Fourier transform, let $\chi_0 \in V$ be the Legendre character and $n = (p-1)/2 = \dim V$. By assumption, the integer n is an

odd prime number. The space V is a hermitian vector space for the ℓ^2 norm and F is a unitary transformation of V.

The following proposition is analogous to Proposition 3.4.*b*.

Proposition 5.1. *Let p be a prime with $p \equiv 3$ mod 4. For all odd Dirichlet character $\chi \neq \chi_0$, the intersection $T \cap F^{-1}T$ is transverse at $[\chi]$.*

Proof of Proposition 5.1. Assume that this intersection $T \cap F^{-1}T$ is not transverse at $[\chi]$. We apply Propositions 3.1 and 3.2. We note that, since the index $n = (p-1)/2$ of H_0 is odd, all the characters $\chi_2 = \psi$ of $\mathbb{F}_p^*/H_0$ have odd order. Therefore the only option among the seven cases of Proposition 3.1 is the first one: the character χ must have order 2. Hence this character is the Legendre character χ_0. □

We recall that T and $T' := F^{-1}T$ are smooth real algebraic subvarieties of $\mathbb{P}(V)$ and that the algebraic multiplicity at $[\chi_0]$ of the intersection $T \cap T'$ is by definition the dimension

$$m_0 := \dim_{\mathbb{C}} A_0. \text{ Here } A_0 \text{ is the local ring } A_0 := \mathcal{A}_0/(\mathcal{I}_0 + \mathcal{I}'_0) \qquad (5.1)$$

where $\mathcal{A}_0$ is the local ring at $[\chi_0]$ of germs of complex valued real analytic functions on $\mathbb{P}(V)$ seen as a real analytic variety, and where $\mathcal{I}_0$ and $\mathcal{I}'_0$ are respectively the ideals of germs of functions that vanish on T and on T' respectively.

Proposition 5.2. *Let $p \geqslant 7$ be a safe prime.*
a) The tori T and $F^{-1}T$ are tangent at $[\chi_0]$ and the algebraic multiplicity at $[\chi_0]$ of the intersection $T \cap F^{-1}T$ is 2^{n-1}.
b) There exist a neighborhood Ω_{χ_0} of $[\chi_0]$ in $\mathbb{P}(V)$ and a continuous family of unitary maps F_t of V with $F_0 = F$ such that, for all $t \in (0,1)$ the intersection $T \cap F_t^{-1}T$ is transverse in Ω_{χ_0} and contains at most 2^{n-2} points in Ω_{χ_0}.

Note that the upper bound of the number of intersection points near $[\chi_0]$ for the perturbation of the Fourier transform is half the algebraic multiplicity at $[\chi_0]$ of this intersection for the Fourier transform.

Proof of Proposition 5.2. It will occupy the rest of Chapter 5.

Proposition 5.2.*a* will follow from Lemma 5.9.

Proposition 5.2.*b* will follow from Lemma 5.12. □

Proof of Theorem 1.2 for a safe prime. Assume, by contradiction that the intersection $T \cap F^{-1}T$ contains only the n points $[\chi]$ associated to the n Dirichlet characters χ that belong to V. We introduce an open neighborhood Ω_{χ_0} of $[\chi_0]$ and a unitary perturbation F_t of the Fourier transform F as in Proposition 5.2. We know that, for all $t \in (0,1)$, the intersection $T \cap F_t^{-1}T$ is transverse in Ω_{χ_0} and contains at most 2^{n-2} points in Ω_{χ_0}.

By Proposition 5.1 the intersection $T \cap F^{-1}T$ is transverse at all the points $[\chi]$ when $\chi \neq \chi_0$. Hence, for $\chi \neq \chi_0$, there also exists a neighborhood Ω_χ of $[\chi]$ in $\mathbb{P}(V)$ such that, if t is small enough, the intersection $T \cap F_t^{-1}T$ is transverse in Ω_χ and contains at most one point in Ω_χ.

One moreover choose t small enough so that the intersection $T \cap F_t^{-1}T$ is included in the union of all the neighborhoods Ω_χ. Then this intersection is transverse and contains at most $2^{n-2}+n-1$ points. Theorem 2.3 predicts the existence of at least 2^{n-1} points in this intersection. Since $n \geqslant 5$, one has $2^{n-1} > 2^{n-2}+n-1$. This is the contradiction we are looking for. □

5.2 A quadratic functional equation

We begin by a crucial lemma that solves a quadratic equation and will allow us to compute the multiplicity in Proposition 5.2.*a*.

Lemma 5.3. *Let p be a safe prime and $\alpha : \mathbb{F}_p \to \mathbb{C}$ be an odd function with*
(i) $\alpha * \alpha = \chi_0 * \chi_0 \alpha^2$,
(ii) $\langle \chi_0, \alpha \rangle = 0$.
Then one has $\alpha = 0$.

Note that if α is an odd function solution of (i), then for all t in $\mathbb{C}$, the odd function $\alpha + t\chi_0$ is also an odd function solution of (i). This is why the linear condition (ii) is natural and useful.

Note also that Equation (i) can be rewritten more explicitely as

$$\sum_{\ell \in \mathbb{F}_p} \alpha_{k-\ell}\alpha_\ell \;=\; \sum_{\ell \in \mathbb{F}_p} \left(\tfrac{k-\ell}{p}\right)\left(\tfrac{\ell}{p}\right) \alpha_\ell^2 \quad \text{for all } k \text{ in } \mathbb{F}_p. \tag{5.2}$$

Note finally that Equation (ii) can be rewritten as,

$$\sum_{\ell \in C} \alpha_\ell \;=\; 0. \tag{5.3}$$

where $C = (\mathbb{F}_p^*)^2$ is the set of non zero squares. Indeed, since $p \equiv 3 \bmod 4$, one has $\mathbb{F}_p^* = C \cup -C$.

Proof. The main trick in the proof is a reduction modulo 2 argument. We first identify the field $\mathbb{C}$ of complex numbers with the algebraic closure $K := \overline{\mathbb{Q}}_2$ of the local field $\mathbb{Q}_2$. We denote by $v_2 : K \to \mathbb{Q} \cup \{+\infty\}$ the 2-adic valuation and by $\mathcal{O}_K = \{\lambda \in K \mid v_2(\lambda) \geqslant 0\}$ the ring of integers of K. It is a local ring whose maximal ideal is $\mathfrak{m}_K := \{\lambda \in K \mid v_2(\lambda) > 0\}$ and whose residual field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ is the algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$.

Let $\alpha : \mathbb{F}_p \to \overline{\mathbb{Q}}_2$ be an odd function satisfying (i) and (ii). We want to prove that $\alpha = 0$. Assume by contradiction that α is non zero. Replacing α by a multiple, one can assume that α takes its values in $\mathcal{O}_K$ and that the reduction $\dot{\alpha} : \mathbb{F}_p \to \overline{\mathbb{F}}_2$ of α modulo $\mathfrak{m}_K$ is non-zero. Since α is odd, one has

$$\dot{\alpha}_0 \;=\; 0 \quad \text{and} \quad \dot{\alpha}_k \;=\; \dot{\alpha}_{-k} \quad \text{for all } k \text{ in } \mathbb{F}_p. \tag{5.4}$$

We write Equation (5.2) with $2k$ instead of k and reduce it modulo 2. On the left hand side, the terms $\dot{\alpha}_{2k-\ell}\dot{\alpha}_\ell$ and $\dot{\alpha}_\ell\dot{\alpha}_{2k-\ell}$ cancel out unless $\ell = k$. On the right hand side, we use the fact that α is odd and that, for $\ell \neq 0$, the legendre symbol $(\frac{\ell}{p})$ is equal to 1 mod 2; when $\ell \neq \pm 2k$, the terms in the sum indexed by ℓ and $-\ell$ cancel out. This gives

$$\dot{\alpha}_k^2 \;=\; \dot{\alpha}_{2k}^2 \quad \text{for all } k \text{ in } \mathbb{F}_p.$$

Since the function $\dot{\alpha}$ takes its values in a field of characteristic 2 this implies

$$\dot{\alpha}_k \;=\; \dot{\alpha}_{2k} \quad \text{for all } k \text{ in } \mathbb{F}_p. \tag{5.5}$$

Reducing Equation (5.3) modulo 2 gives

$$\sum_{\ell \in C} \dot{\alpha}_\ell \;=\; 0. \tag{5.6}$$

Since the integer $(p-1)/2$ is prime, the group $\mathbb{F}_p^*$ is generated by the two elements -1 and 2. Therefore, Equations (5.4) and (5.5) tell us that the function $\dot{\alpha}$ is constant equal to $\dot{\alpha}_1$ outside 0. Since the cardinality of C is odd, plugging this information into (5.6) gives $\dot{\alpha}_1 = 0$, and therefore $\dot{\alpha} = 0$. This is a contradiction. □

5.3 Multiplicity of holomorphic maps

In this section, we recall a few general definitions and facts that deal with the topological degree of a proper holomorphic map with finite fibers.

For $\Omega \subset \mathbb{C}^m$ an open set, $\Psi_0 : \Omega \to \mathbb{C}^m$ a holomorphic map and $z \in \Omega$ such that $\Psi_0(z) = 0$, we recall that the *algebraic multiplicity* $m_z(\Psi_0)$ is the dimension of the local ring $\mathcal{O}_z/\Psi_0^*\mathcal{O}_0$ where $\mathcal{O}_z$ is the local ring of germs at z of holomorphic functions and where $\Psi_0^*\mathcal{O}_0$ is the ideal spanned by the functions $h\circ\Psi_0$ where h is a holomorphic function that vanishes at 0. A point $z_0 \in \Omega$ is a *critical point* for Ψ_0 if and only if the tangent map $D\Psi_0(z_0)$ is not invertible, or equivalently $m_{z_0}(\Psi_0 - f(z_0)) > 1$. A *critical value* for Ψ_0 is the image $\Psi_0(z_0)$ of a critical point z_0. A *regular value* is a value which is not critical. By Sard theorem, the set of critical values has Lebesgue measure 0. When the algebraic multiplicity $m_z(\Psi_0)$ is finite it coincides with the *geometric multiplicity*. This means that, there exists $\varepsilon_0 > 0$ and a neighborhood Ω_0 of z such that for Lebesgue almost all $w \in \mathbb{C}^m$ with $\|w\| < \varepsilon_0$, the value w is a regular value of $\Psi_0 - w$ and one has $m_z(\Psi_0) = \#(\Psi_0^{-1}(w) \cap \Omega_0)$. See [1, Ch.1 prop. 2.1] and [34, p.148].

The first fact extends to several variables the famous Rouché theorem.

Fact 5.4. *Let $\Omega \subset \mathbb{C}^m$ be an open set, let $\overline{B} \subset \Omega$ be a compact ball and $I \subset \mathbb{R}$ be an interval. Let $(\Psi_t)_{t\in I}$ be a continuous family of holomorphic map $\Psi_t : \Omega \to \mathbb{C}^m$ such that for all t in I, the function Ψ_t does not vanish on the boundary ∂B. Then the number of zeros of Ψ_t in $\overline{B}$ counted with multiplicities : $\sum_{\{z\in\overline{B}|\Psi_t(z)=0\}} m_z(\Psi_t)$ does not depend on t.*

Proof. See [1, Thm 2.5]. □

The second fact explains how to compute the algebraic multiplicity for a complete intersection quadratic map. It also explains why in some fibers at most half of the points are real.

Fact 5.5. *Let $Q = (Q_1, \dots, Q_m) : \mathbb{C}^m \to \mathbb{C}^m$ be a homogeneous polynomial map of degree 2 which is anisotropic over $\mathbb{C}$ i.e. such that $Q^{-1}(0) = \{0\}$.*
a) Then there exists $C > 0$ such that, for all $z \in \mathbb{C}^m$, one has

$$C^{-1}\|z\|^2 \leqslant \|Q(z)\| \leqslant C\|z\|^2.$$

b) The algebraic multiplicity of Q at 0 is $m_0(Q) = 2^m$.
c) For all $w \neq 0$ in $\mathbb{C}^m$, there exists a sign $\varepsilon = \pm 1$ such that

$$\#(Q^{-1}(\varepsilon w) \cap \mathbb{R}^m) \ \leqslant \ 2^{m-1}.$$

Proof. *a*) These inequalities follow from the homogeneity of Q by choosing the constant C to be $C = \max_{\|z\|=1} \max(\|Q(z)\|, \|Q(z)\|^{-1})$.

b) According to [34, p.142], since Q is anisotropic, the multiplicity of Q at 0 is equal to the product of the degrees of the homogeneous polynomials Q_j which is 2^m.

c) Remember the equality $Q(iz) = -Q(z)$, for all z in $\mathbb{C}^m$. For $w \neq 0$, the set $Q^{-1}(w) \cup Q^{-1}(-w)$ contains at most 2^{m+1} points and is stable by multiplication by i. Therefore it contains at most 2^m real points and one of these two fibers $Q^{-1}(\varepsilon\, w)$ contains at most 2^{m-1} real points. □

Remark 5.6. We will not need it, but one can say much more: the quotient algebra $A_0 := \mathbb{C}[z_1, , z_m]/\langle Q_1, \ldots, Q_m\rangle$ is a finite graded commutative $\mathbb{C}$-algebra whose Hilbert polynomial is $P_{A_0}(t) = (1+t)^m$. Moreover this local algebra A_0 is a "complete intersection algebra", hence a "Poincaré duality algebra" and a "Cohen-Macauley algebra". These facts follow from the Macaulay theorem and the Koszul theorem (see [30, thm 6.7.6 and 6.2.4]).

The third fact tells us that one can sometimes reduce the calculation of the algebraic multiplicity to the previous example.

Fact 5.7. *Let $\Omega \subset \mathbb{C}^m$ be an open set containing 0 and $\Psi_0 : \Omega \to \mathbb{C}^m$ be a holomorphic map such that $\Psi_0(0) = 0$ and $D\Psi_0(0) = 0$. Assume that the Hessian $Q := \frac{1}{2}D^2\Psi_0(0) : \mathbb{C}^m \to \mathbb{C}^m$ is an anisotropic quadratic map.*
a) Then there exist $\varepsilon_0 > 0$, $C > 0$ such that, for $z \in \mathbb{C}^m$ with $\|z\| \leqslant \varepsilon_0$,

$$C^{-1}\|z\|^2 \leqslant \|\Psi_0(z)\| \leqslant C\|z\|^2.$$

b) The algebraic multiplicity of Ψ_0 at 0 is $m_0(\Psi_0) = 2^m$.

Proof. *a*) We write $\Psi_0(z) = Q(z) + R(z)$ where $Q : \mathbb{C}^m \to \mathbb{C}^m$ is a quadratic polynomial map and where $\lim_{z\to 0} \frac{\|R(z)\|}{\|z\|^2} = 0$. We apply then Fact (5.5).*a*.

b) According to [34, p.146], since Q is anisotropic, the multiplicity of Ψ_0 at 0 is equal to the multiplicity of Q at 0 which is 2^m. □

5.4 Multiplicity of $T \cap F^{-1}T$ at the Legendre character

We come back to the notation of Sections 5.1 and 5.2. The aim of this section is to apply the general results of Section 5.3 to determine the multiplicity of the intersection $T \cap F^{-1}T$ at the point $[\chi_0]$ given by the Legendre character χ_0.

We introduce the complex vector spaces

$$\begin{aligned} V_0 &= \{\alpha : \mathbb{F}_p \to \mathbb{C} \mid \alpha \text{ is odd and } \langle \chi_0, \alpha \rangle = 0\}, \\ W_0 &= \{\beta : \mathbb{F}_p \to \mathbb{C} \mid \beta \text{ is even and } \beta(0) = \widehat{\beta}(0) = 0\}. \end{aligned}$$

Note that these two vector spaces have dimension $n-1 = (p-3)/2$ and that the formula $\alpha = \chi_0 \beta$ induces an isomorphism between V_0 and W_0.

It will be convenient to use a parametrization of a neighborhood of $[\chi_0]$ in $\mathbb{P}(V)$ by the ball

$$B_0 = \{\beta \in W_0 \mid \|\beta\|_\infty < \pi/2\}.$$

This parametrization is given by

$$\beta \mapsto [f_\beta] \text{ where } f_\beta = \chi_0 \, e^{i\beta}. \tag{5.7}$$

The next lemma describes T and $F^{-1}T$ via this parametrization. We set

$$V_{0,\mathbb{R}} = \{\alpha \in V_0 \mid \alpha = \overline{\alpha}\}, \; W_{0,\mathbb{R}} = \{\beta \in W_0 \mid \beta = \overline{\beta}\} \text{ and } B_{0,\mathbb{R}} = B_0 \cap W_{0,\mathbb{R}}.$$

Lemma 5.8. *a) The following map $\Psi_0 : W_0 \to W_0$ is well defined*

$$\beta \mapsto \Psi_0(\beta) := \chi_0 e^{i\beta} * \chi_0 e^{-i\beta} - \chi_0 * \chi_0 \, . \tag{5.8}$$

b) For β in B_0, one has the equivalences: $\chi_0 e^{i\beta} \in T \iff \beta = \overline{\beta}$ and $\chi_0 e^{i\beta} \in F^{-1}T \iff \chi_0 e^{i\beta} * \chi_0 e^{-i\overline{\beta}} = \chi_0 * \chi_0$.
c) The multiplicity m_0 of the intersection $T \cap F^{-1}T$ at $[\chi_0]$ is equal to the algebraic multiplicity $m_0(\Psi_0)$ of Ψ_0 at 0.

Note that, since $p \equiv 3 \bmod 4$, one has $\chi_0 * \chi_0 = \mathbf{1}_{\mathbb{F}_p} - p\,\delta_0$.

Proof. *a)* We want to check that, for β in W_0, the function $\Psi_0(\beta)$ also belongs to W_0. Since $p \equiv 3 \bmod 4$, the Legendre character χ_0 is odd and the functions $\chi_0 e^{\pm i\beta}$ are also odd. Therefore the function $\Psi_0(\beta)$ is even.
Since the function β is even, one has

$$\Psi_0(\beta)(0) = \sum_{k \in \mathbb{F}_p} (\chi_0(k) e^{i\beta(k)} \chi_0(-k) e^{-i\beta(-k)} - \chi_0(k)\chi_0(-k)) = 0$$

Since the functions $f_\beta = \chi_0 e^{i\beta}$ is odd, one has

$$\tfrac{1}{\sqrt{p}} \widehat{\Psi_0(\beta)}(0) = \widehat{f_\beta}(0) \, \widehat{f_{-\beta}}(0) - (\widehat{\chi_0}(0))^2 = 0$$

This proves that the function $\Psi_0(\beta)$ belongs to W_0.

b) The first equivalence follows from the definition. The proof of the second equivalence is similar to the proof of Lemma 2.4.

c) In the coordinate system $\beta \mapsto [f_\beta]$ as in (5.7), the components of the real analytic map $\beta \mapsto \beta - \overline{\beta}$ spans the ideal of germs at $[\chi_0]$ of real analytic functions that vanish on T. Similarly, the components of the real analytic map $\beta \mapsto \chi_0 e^{i\beta} * \chi_0 e^{-i\overline{\beta}} - \chi_0 * \chi_0$ spans the ideal of germs at 0 of real analytic functions that vanish on $F^{-1}T$. Therefore the local ring A_0 at $[\chi_0]$ of the schematic intersection $T \cap F^{-1}T$ defined in (5.1) is isomorphic to $\mathcal{O}_0/\Psi_0^*(\mathcal{O}_0)$ where $\mathcal{O}_0$ is the ring of germs at 0 of holomorphic functions on W_0. The dimension of this ring is $m_0(\Psi_0)$. □

We check now that this map Ψ_0 satisfies the assumptions of Fact 5.7

Lemma 5.9. *The holomorphic map Ψ_0 given by* (5.8) *satisfies:*
(*i*) *at the point* 0, *the map Ψ_0 vanishes: $\Psi_0(0) = 0$.*
(*ii*) *the differential $D\Psi_0(0) : W_0 \to W_0$ vanishes: $D\Psi_0(0) = 0$,*
(*iii*) *the hessian $Q = \frac{1}{2}D^2\Psi_0(0) : W_0 \to W_0$ is an anisotropic quadratic map.*
And therefore the multiplicity $m_0 = m_0(\Psi_0)$ is equal to 2^{n-1}.

Remark 5.10. The assertion (*ii*) reflects the fact that the Clifford tori T and $F^{-1}T$ are tangent at the point $[\chi_0]$.

Proof. One computes, for β in W_0, using Formula (5.8):

$$\begin{aligned} \Psi_0(0) &= \chi_0 * \chi_0 - \chi_0 * \chi_0 = 0, \\ D\Psi_0(0)(\beta) &= i\chi_0\beta * \chi_0 - i\chi_0 * \chi_0\beta = 0, \\ Q(\beta) = \tfrac{1}{2}D^2\Psi_0(0)(\beta) &= \chi_0\beta * \chi_0\beta - \chi_0 * \chi_0\beta^2. \end{aligned}$$

According to Lemma 5.3 this quadratic map Q is anisotropic. Therefore, we can apply Fact 5.7 to the holomorphic map Ψ_0 and the multiplicity of Ψ_0 at 0 is equal to 2^m where $m = \dim_{\mathbb{C}} W_0 = n-1 = (p-3)/2$. □

5.5 Moving slightly the torus

The aim of this section is to prove Proposition 5.2, that is to find a small unitary deformation F_t of the Fourier transform F such that the intersection $T \cap F_t^{-1}T$ is transverse and contains at most 2^{n-2} points.

In order to clarify our arguments, we begin by a general result that deal with analytic families of real analytic maps.

Lemma 5.11. *Let $I \subset \mathbb{R}$ and $\Omega \subset \mathbb{C}^m$ be two open sets containing 0, and let $\Psi : I \times \Omega \to \mathbb{C}^m; (t, z) \mapsto \Psi_t(z)$ be a real analytic family of holomorphic maps such that*
(i) the value $\Psi_0(0)$ vanishes: $\Psi_0(0) = 0$,
(ii) the differential $D\Psi_0(0) : \mathbb{C}^m \to \mathbb{C}^m$ vanishes: $D\Psi_0(0) = 0$,
(iii) the hessian $Q := \frac{1}{2}D^2\Psi_0(0) : \mathbb{C}^m \to \mathbb{C}^m$ is anisotropic: $Q^{-1}(0) = \{0\}$,
(iv) the element $w_0 := -\frac{d}{dt}\Psi_t(0)|_{t=0} \in \mathbb{C}^m$ is a regular value of Q.
Then there exists $t_0 > 0$, a radius $\rho_0 > 0$ and a sign $\varepsilon = \pm 1$ such that, for all t in $(0, t_0)$, the point 0 is a regular value for the restriction of $\Psi_{\varepsilon t}$ to the ball $B_{\mathbb{R}^m}(0, \rho_0)$ and one has

$$\#(\Psi_{\varepsilon t}^{-1}(0) \cap B_{\mathbb{R}^m}(0, \rho_0)) \;\leqslant\; 2^{m-1}. \tag{5.9}$$

Here $B_{\mathbb{R}^m}(0, \rho_0)$ is the ball in $\mathbb{R}^m$ with center 0 and radius ρ_0, and the bound (5.9) is a control on the number of real points near 0 in the fiber $\Psi_{\varepsilon t}^{-1}(0)$ by half the multiplicity of Ψ_0 at 0.

Proof. According to Fact 5.5, there exists a sign $\varepsilon = \pm 1$ such that

$$\#(Q^{-1}(\varepsilon\, w_0) \cap \mathbb{R}^m) \;\leqslant\; 2^{m-1}. \tag{5.10}$$

Note that, since $Q(iz) = -Q(z)$, the value $-w_0$ is also regular for Q. Without loss of generality, we can reverse the time and assume that $\varepsilon = 1$.

We want to describe the fiber $\Psi_t^{-1}(0)$ near 0, for $t > 0$ small. The assumptions (i), (ii) and (iii) tell us that one can write in a unique way

$$\Psi_t(z) \;=\; \Psi_t(0) + Q(z) + R(z) + t\, r_t(z) \tag{5.11}$$

where R and r_t are holomorphic maps from Ω to $\mathbb{C}^m$ with

$$R(z) = o(\|z\|^2) \;\text{ and }\; r_t(0) = 0\,.$$

Since w_0 is a regular value for Q, by Fact 5.4 and 5.5, there exist 2^m distinct points $v_k \in \mathbb{C}^m$ indexed by $k = 1, \ldots, 2^m$ such that

$$Q(v_k) \;=\; w_0 \quad\text{and}\quad J_Q(v_k) \;\neq\; 0\,,$$

where $J_Q(z) = \det(DQ(z)) \in \mathbb{C}$ is the Jacobian of the holomorphic map Q. We set $M_0 := \max\limits_{k \leqslant 2^m} \|v_k\| + 1$.

Since the map Ψ is singular at the point $(0,0)$, it will be useful to introduce the auxiliary map $\Phi : (-s_0, s_0) \times B_{\mathbb{C}^m}(0, M_0) \to \mathbb{C}^m$ given by

$$\begin{aligned} \Phi_s(v) &= \Psi_{s^2}(s\,v)/s^2 \quad \text{when } s \neq 0 \\ &= Q(v) - w_0 \text{ when } s = 0. \end{aligned}$$

When $s_0 > 0$ is chosen small enough, this map Φ is well defined and $s \mapsto \Phi_s$ is an analytic family of holomorphic maps. Indeed, by (5.11), one has

$$\begin{aligned} \Phi_s(v) &= \Psi_{s^2}(0)/s^2 + Q(v) + R(sv)/s^2 + r_{s^2}(sv) \quad \text{when } s \neq 0 \\ &= -w_0 + Q(v) + 0 + 0 \qquad \text{when } s = 0, \end{aligned}$$

and each of the four terms is an analytic family of holomorphic maps.

By construction one has

$$\Phi_0^{-1}(0) = Q^{-1}(w_0) = \{v_k \mid k = 1, \dots, 2^m\}.$$

This map Φ is particulaly useful since, by the assumption (iv), for all $k \leqslant 2^m$ the differentials $D\Phi_0(v_k) = DQ(v_k)$ are invertible. This means that 0 is a regular value of the map Φ_0.

By the implicit function theorem, there exists $s_0' > 0$, such that, for all $k \leqslant 2^m$, there exist analytic maps $\varphi_k : (-s_0', s_0') \to \mathbb{C}^m$ satisfying

$$\varphi_k(0) = v_k \quad \text{and} \quad \Phi_s(\varphi_k(s)) = 0 \text{ for all } s \in (-s_0', s_0'). \tag{5.12}$$

Fix a radius $\rho_0 < d(0, \partial\Omega)$. According to Fact 5.4, for $t > 0$ small enough the fiber $\Psi_t^{-1}(0)$ contains at most 2^m points in the complex ball $B_{\mathbb{C}^m}(0, \rho_0)$. By (5.12), these points are exactly the points

$$z_k(t) := t^{1/2}\varphi_k(t^{1/2}).$$

For t small enough, the point $z_k(t)$ is real if and only if v_k is real. By (5.10), among these 2^m points v_k, at most 2^{m-1} points are real. This proves the bound (5.9). □

We now come back to the notation of Section 5.4. We want to construct the unitary deformation F_t of the Fourier transform F.

We introduce the group $U(V) \simeq U(n, \mathbb{R})$ of unitary transformations of $V \simeq \mathbb{C}^n$ and its Lie algebra

$$\mathfrak{u}(V) := \{X_0 \in \mathrm{End}(V) \mid X_0 \text{ is antihermitian}\}.$$

We introduce the euclidean space $V_{\mathbb{R}} := \{f \in V \mid \overline{f} = f\} \simeq \mathbb{R}^n$, the orthogonal group $O(V_{\mathbb{R}}) := \{u \in U(V) \mid \overline{u} = u\} \simeq O(n, \mathbb{R})$ and its Lie algebra

$$\mathfrak{o}(V_{\mathbb{R}}) \ := \ \{X_0 \in \mathfrak{u}(V) \mid \overline{X_0} = X_0\}.$$

We fix an element $X_0 \in \mathfrak{o}(V_{\mathbb{R}})$ and we introduce the analytic family

$$F_t := F \circ e^{tX_0}$$

of unitary deformations of the Fourier transform $F = F_0$.

The following lemma introduces an analytic family Ψ_t of holomorphic maps of $W_0 \simeq \mathbb{C}^{n-1} = \mathbb{C}^{(p-3)/2}$ which is useful. Here is why.
$\star$ On the one hand the fiber $\Psi_t^{-1}(0)$ near 0 parametrizes $T \cap F_t^{-1}T$ near $[\chi_0]$ in the coordinate system (5.7), for t small.
$\star$ On the other hand the family Ψ_t satisfies the assumptions $(i) - (iv)$ of Lemma 5.11, provided X_0 is well chosen.

Lemma 5.12. *a) The following map $\Psi : \mathbb{R} \times W_0 \to W_0$ is well defined*

$$(t, \beta) \mapsto \Psi_t(\beta) := \ e^{tX_0}(\chi_0 e^{i\beta}) \ * \ e^{tX_0}(\chi_0 e^{-i\beta}) \ - \ \chi_0 * \chi_0 \, .$$

b) For $t \in \mathbb{R}$ and $\beta \in B_{0,\mathbb{R}}$, one has the equivalence:

$$\chi_0 e^{i\beta} \in F_t^{-1}T \Longleftrightarrow \Psi_t(\beta) = 0.$$

c) One can choose $X_0 \in \mathfrak{o}(\mathbb{R})$ such that the derivative $w_0 := -\frac{d}{dt}\Psi_t(0)|_{t=0}$ is a regular value for the Hessian $Q := \frac{1}{2}D^2\Psi_0(0)$.
d) With this choice, the family Ψ_t satisfies the assumptions (i)–(iv) of Lemma 5.11. In particular there exist a neighborhood Ω_{χ_0} of $[\chi_0]$ in $\mathbb{P}(V)$ and a sign $\varepsilon = \pm 1$ such that, for all $t \in (0, 1)$ the intersection $T \cap F_{\varepsilon t}^{-1}T$ is transverse in Ω_{χ_0} and contains at most 2^{n-2} points in Ω_{χ_0}.

Proof. *a*) The proof is as in Lemma 5.8.*a*. We want to check that, for β in W_0, the function $\Psi_t(\beta)$ also belongs to W_0. Since the functions $f_{\pm\beta} = \chi_0 e^{\pm i\beta}$ are odd, the functions $e^{tX_0}f_{\pm\beta}$ are also odd and the function $\Psi_t(\beta)$ is even. Moreover, since the unitary map e^{tX_0} is orthogonal, one also has

$$\Psi_t(\beta)(0) \ = \ -\|e^{tX_0}f_\beta\|_{\ell^2}^2 + \|\chi_0\|_{\ell^2}^2 \ = \ -\|f_\beta\|_{\ell^2}^2 + \|\chi_0\|_{\ell^2}^2 \ = \ 0$$

Since the function $e^{tX_0}f_\beta$ and its Fourier transform $\widehat{e^{tX_0}f_\beta}$ are odd, one has

$$\tfrac{1}{\sqrt{p}}\,\widehat{\Psi_t(\beta)}(0) \ = \ \widehat{e^{tX_0}f_\beta}(0)\,\widehat{e^{tX_0}f_{-\beta}}(0) \ - \ (\widehat{\chi_0}(0))^2 \ = \ 0$$

This proves that the function $\Psi_t(\beta)$ belongs to W_0.

b) The proof is as in Lemma 5.8.*b*.

c) This follows from the following four assertions:
The derivative w_0 is equal to $w_0 = -2\, X_0(\chi_0) * \chi_0$.
The map $\mathfrak{o}(V_{\mathbb{R}}) \to V_{0,\mathbb{R}}; X_0 \mapsto \alpha := X_0(\chi_0)$ is onto.
The map $V_{0,\mathbb{R}} \to W_{0,\mathbb{R}}; \alpha \mapsto \beta := \alpha * \chi_0$ is an isomorphism.
The real vector space $W_{0,\mathbb{R}}$ is not contained in the set $Z \subset W_0$ of singular values of the holomorphic quadratic map $Q : W_0 \to W_0$.

d) The first statement follows from Point *c*) and from Lemma 5.9. The last statement follows from Point *b*) and from Lemma 5.11. □

This ends the proof of Proposition 5.2 and hence this also ends the proof of Theorem 1.2.

6 Counting $\mathcal{C}$-functions

The aim of this Chapter is to prove Theorem 6.6 which is an extension of Theorem 1.3. This extension gives a formula for the number of (H, c)-equivariant $\mathcal{C}$-functions.

In Section 6.1, we give a short and new proof of the finiteness of the set of $\mathcal{C}$-functions f with $f(1) = 1$.

In Section 6.2, we explain the deformation argument that allows one to compute the number of (H, c)-equivariant $\mathcal{C}$-functions.

6.1 Finiteness of the set of $\mathcal{C}$-functions

The following proposition is due to Biro.

Proposition 6.1. ([7]) *Let p be a prime number. Then the set of $\mathcal{C}$-functions f on $\mathbb{F}_p$ such that $f(1) = 1$ is finite.*

We will give a different proof of this proposition whose arguments will be reused in the sequel. We first recall a lemma due to Chebotarev that we call the little Chebotarev theorem.

Lemma 6.2. ([31]) *Let p be a prime number and $\zeta_p := e^{2i\pi/p}$. For any subset A, B of $\mathbb{F}_p$ with same cardinality, the matrix $(\zeta_p^{jk})_{\substack{j\in A\\ k\in B}}$ is invertible*

The little theorem of Chebotarev has been reinterpreted by Biro and Tao as the following equivalent statement.

Lemma 6.3. (see [8, p.2] and [32]) *Let p be a prime number. For every non zero function f on $\mathbb{F}_p$, one has*

$$\#\operatorname{supp}(f) + \#\operatorname{supp}(\widehat{f}) \;\geqslant\; p+1\,. \tag{6.1}$$

This lemma is the key ingredient towards the following proposition due to Haagerup. Let $E = \mathbb{C}^{\mathbb{F}_p}$ be the set of functions on $\mathbb{F}_p$ endowed with the sup-norm $\|.\|_\infty$ and $E_{\geqslant 1}$ be the complementary of the open ball of radius 1,

$$E_{\geqslant 1} := \{f \in E \mid \|f\|_\infty \geqslant 1\}.$$

Proposition 6.4. ([18]) *Let p be a prime number. Then the map*

$$\begin{array}{rcl} \Phi : E_{\geqslant 1} \times E_{\geqslant 1} & \longrightarrow & E \times E \\ (f,g) & \mapsto & (fg, \widehat{f}\,\widehat{\breve{g}}) \end{array}$$

is a proper map.

"Proper" means that the inverse image of a compact set is compact.

Remark 6.5. The same would be true with the map $\Psi : (f,g) \mapsto (fg, \widehat{f}\,\widehat{g})$. But the map Φ wich involves $\breve{g}$ is more useful for us because of Lemma 2.4.

Proof of Proposition 6.4. Assume by contradiction that there exists sequences f_n, g_n in $E_{\geqslant 1}$ with $\max(\|f_n\|_\infty, \|g_n\|_\infty)$ going to ∞ such that $\Phi(f_n, g_n)$ converges. After extracting a subsequence, the renormalized functions converge

$$u_n := \frac{f_n}{\|f_n\|_\infty} \to u_\infty \;\text{ and }\; v_n := \frac{g_n}{\|g_n\|_\infty} \to v_\infty\,,$$

and the limit functions u_∞ and v_∞ are non zero functions. Since the product $\|f_n\|_\infty \|g_n\|_\infty$ goes to ∞, these limits satisfy

$$u_\infty v_\infty = 0 \;\text{ and }\; \widehat{u}_\infty \widehat{\breve{v}}_\infty = 0.$$

In particular, one has the inequality

$$\#\operatorname{supp}(u_\infty) + \#\operatorname{supp}(v_\infty) + \#\operatorname{supp}(\widehat{u}_\infty) + \#\operatorname{supp}(\widehat{v}_\infty) \;\leqslant\; 2p,$$

which contradicts Lemma 6.3. □

Proof of Proposition 6.1. We introduce the complex affine subspace of dimension $p-2$ in $E := \mathbb{C}^{\mathbb{F}_p}$,

$$E_1 := \{f \in \mathbb{C}^{\mathbb{F}_p} \mid f(0) = 0 \text{ and } f(1) = 1\},$$

We have seen in Proposition 6.4 that the map

$$\begin{aligned} \Phi : E_1 \times E_1 &\longrightarrow E \times E && (6.2)\\ (f, g) &\mapsto (fg, \widehat{f}\widehat{g}) && (6.3) \end{aligned}$$

is a proper map. By Lemma 2.4, a function f in F_1 is a $\mathcal{C}$-function if and only if there exists a (unique) function g in E_1 such that $\Phi(f, g) = (\mathbf{1}_{\mathbb{F}_p^*}, \mathbf{1}_{\mathbb{F}_p^*})$. By Proposition 6.4 the complex algebraic subvariety $\Phi^{-1}(\mathbf{1}_{\mathbb{F}_p^*}, \mathbf{1}_{\mathbb{F}_p^*})$ of $E_1 \times E_1$ is compact. Therefore it is finite. □

6.2 Counting equivariant $\mathcal{C}$-functions

We want to prove the following.

Theorem 6.6. *Let p be an odd prime, $H \subset \mathbb{F}_p^*$ be a subgroup of index n, and $c : H \to \mathbb{C}^*$ be a non-trivial character. Then, counted with multiplicities, the number of (H, c)-equivariant $\mathcal{C}$-functions f on $\mathbb{F}_p$ with $f(1) = 1$, is equal to the binomial coefficient $\binom{2n-2}{n-1}$.*

Proof of Theorem 1.3. Just apply Theorem 6.6 with the group $H = \{\pm 1\}$ and with the unique odd character c of H. The (H, c)-equivariant functions f are nothing but the odd $\mathcal{C}$-functions and the index n is $n = (p-1)/2$. □

The key point will be a deformation argument. For this argument one needs a defining map Φ as in (6.2) which is not only proper but also dominant so that the number of points in its fibers, counted with multiplicities is constant, and so that we can perform the counting for a simpler fiber.

We introduce the vector space $V = V_{H,c}$ of (H, c)-equivariant functions f on $\mathbb{F}_p$ as in (3.7), and its affine subspace

$$V_1 := \{f \in V_{H,c} \mid f(1) = 1\}.$$

Since c is non trivial, all these (H, c)-equivariant functions vanish at 0. The conjugate affine space is

$$\overline{V}_1 := \{g \in V_{H,\bar{c}} \mid g(1) = 1\}.$$

We also introduce the space V_0 of H-invariant functions f_0 on $\mathbb{F}_p$ such that $f_0(0) = 0$, and the affine space

$$W_1 := \{(f_0, g_0) \in V_0 \times V_0 \mid f_0(1) = 1 \text{ and } \sum_{x\in\mathbb{F}_p} f_0(x) = \sum_{x\in\mathbb{F}_p} g_0(x) \}.$$

Lemma 6.7. *The map*

$$\begin{array}{rcl} \Phi : V_1 \times \overline{V}_1 & \longrightarrow & W_1 \\ (f, g) & \mapsto & (fg, \widehat{f}\,\widehat{\overline{g}}) \end{array} \tag{6.4}$$

is a well-defined dominant and proper map.

Note that $\dim(W_1) = 2\dim(V_1) = 2n - 2$.

Proof of Lemma 6.7. We first check that $\Phi(V_1 \times \overline{V}_1)$ is included in W_1. Let f be in V_1, let g be in $\overline{V}_1$. Since f is (H, c) equivariant and g is $(H, \overline{c})$-equivariant, the function fg is H-invariant and vanish at 0. Similarly, since $\widehat{f}$ is $(H, \overline{c})$ equivariant and $\widehat{\overline{g}}$ is (H, c)-equivariant, the function $\widehat{f}\,\widehat{\overline{g}}$ is H-invariant and vanish at 0. Since $f(1) = g(1) = 1$, one also has $fg(1) = 1$ The last equality $\sum_{x\in\mathbb{F}_p} fg(x) = \sum_{x\in\mathbb{F}_p} \widehat{f}\,\widehat{\overline{g}}(x)$ is the Parseval formula for finite Fourier transform.

The fact that the map Φ is proper follows from Proposition 6.4.

The fact that Φ is dominant follows from properness and equidimensionality. One can also exhibit an explicit point (f, g) at which the differential $D\Phi(f, g)$ is an isomorphism. For instance the points in Lemma 6.8.*e*. □

In the following lemma we study in great detail the fiber of Φ over the point $(\mathbf{1}_H, \mathbf{1}_H)$.

Lemma 6.8. *Let H be a subgroup of $G := \mathbb{F}_p^*$ and c be a non trivial character of H. Let Φ be the map* (6.4).
a) For every H-invariant subsets A, B of $\mathbb{F}_p^*$ containing H such that

$$\#A + \#B = \#G + \#H, \tag{6.5}$$

there exists a unique function $f_{A,B} \in V_1$ with support A whose Fourier transform $\widehat{f}_{A,B} \in V_{H,\overline{c}}$ has support B.
b) We set $g_{A,B} \in \overline{V}_1$ to be the function $g_{A,B} := \overline{f}_{A',-B'}$ where A' and B' are defined by $A \cup A' = B \cup B' = G$ and $A \cap A' = B \cap B' = H$. Then one has

$$\Phi(f_{A,B}, g_{A,B}) = (\mathbf{1}_H, \mathbf{1}_H).$$

c) Every point in the fiber $\Phi^{-1}(\mathbf{1}_H, \mathbf{1}_H)$ is one of these points $(f_{A,B}, g_{A,B})$.
d) The number of points in this fiber $\Phi^{-1}(\mathbf{1}_H, \mathbf{1}_H)$ is equal to $\binom{2n-2}{n-1}$.
e) The map Φ is non-degenerate at the points $(f_{A,B}, g_{A,B})$ of this fiber.

Proof of Lemma 6.8. Let $d = p-1$, and write $d = n\, d_H$ where n is the index of H and d_H the order of H.

a) For a H-invariant subset A of G of cardinality $n_A d_H$, we denote by $\mathbb{C}[A]_{H,c}$ the vector space of (H,c)-equivariant functions on A. It has dimension n_A.

As a consequence of Inequality (6.1), for any H-invariant subsets A_0 and B_0 of G with $n_{A_0} + n_{B_0} = n$, the map

$$\mathbb{C}[A_0]_{H,c} \to \mathbb{C}[B_0^c]_{H,\overline{c}} : f \to \widehat{f}|_{B_0^c}$$

is an isomorphism.

Therefore, for any H-invariant subsets A and B of G with $n_A + n_B = n+1$, the map

$$\mathbb{C}[A]_{H,c} \to \mathbb{C}[B^c]_{H,\overline{c}} : f \to \widehat{f}|_{B^c}$$

has a one dimensional kernel. Moreover, a non-zero function $f_{A,B}$ in the kernel does not vanish on A; one can normalize it so that $f_{A,B}(1) = 1$. Similarly its Fourier transform $\widehat{f}_{A,B}$ does not vanish on B.

b) Let $f := f_{A,B}$ and $g := g_{A,B}$. By construction the product fg is H-invariant, is supported by H and satisfies $fg(1) = 1$. Therefore one has $fg = \mathbf{1}_H$.

Similarly the product $\widehat{f}\widehat{g}$ is H-invariant and is supported by H. Therefore one has $\widehat{f}\widehat{g} = \lambda \mathbf{1}_H$ for some constant λ. This constant λ is equal to 1 by the Parseval-Plancherel formula.

c) Conversely, let $(f,g) \in V_1 \times \overline{V}_1$ such that $fg = \mathbf{1}_H$ and $\widehat{f}\widehat{g} = \mathbf{1}_H$. Set $A := \mathrm{supp}(f)$, $B := \mathrm{supp}(\widehat{f})$, $A' := \mathrm{supp}(g)$ and $B' := \mathrm{supp}(\widehat{g})$. By assumption, one has $A \cap A' = B \cap B' = H$. In particular, one has

$$n_A + n_{A'} \leqslant n+1 \ \text{ and } \ n_B + n_{B'} \leqslant n+1.$$

By inequality (6.1), one has

$$n_A + n_B \geqslant n+1 \ \text{ and } \ n_{A'} + n_{B'} \geqslant n+1.$$

Therefore all these inequalities are equalities and hence, by point *a)*, one has $f = f_{A,B}$ and $g = \overline{f}_{A',-B'} = g_{A,B}$.

d) By Point *c*), the fiber $\Phi^{-1}(\mathbf{1}_H, \mathbf{1}_H)$ is in bijection with the set of pairs $(A \smallsetminus H, B \smallsetminus H)$ of H-invariant subsets of $G \smallsetminus H$ such that $n_{A \smallsetminus H} + n_{B \smallsetminus H} = n-1$. Their total number is $\binom{2n-2}{n-1}$ as announced.

e) Fix a point $(f, g) = (f_{A,B}, \overline{f}_{A',-B'})$ in the fiber $\Phi^{-1}(\mathbf{1}_H, \mathbf{1}_H)$. We want to prove that the differential $D\Phi(f, g)$ is injective. The tangent space of the source is the space of couples (φ, ψ) of (H, c)-equivariant functions such that $\varphi(1) = \psi(1) = 0$. Assume that (φ, ψ) is in the kernel of $D\Phi(f, g)$. The formula for the differential is

$$D\Phi(f, g)(\varphi, \psi) = (f\psi + g\varphi, \widehat{f}\widehat{\psi} + \widehat{\overline{g}}\widehat{\varphi}) = 0.$$

Since the functions $f\psi$ is supported by $A \smallsetminus H$ and the function $g\varphi$ is supported by $A' \smallsetminus H$, one gets $f\psi = g\varphi = 0$. Since f does not vanish on A and g does not vanish on A', this proves that

$$\mathrm{supp}(\varphi) \subset A \smallsetminus H \ \text{ and } \ \mathrm{supp}(\psi) \subset A' \smallsetminus H.$$

A similar argument proves that $\widehat{f}\widehat{\psi} = \widehat{\overline{g}}\widehat{\varphi} = 0$ and that

$$\mathrm{supp}(\widehat{\varphi}) \subset B \ \text{ and } \ \mathrm{supp}(\widehat{\psi}) \subset -B'.$$

In particular one gets

$$\begin{aligned} \#\mathrm{supp}(\varphi) + \#\mathrm{supp}(\widehat{\varphi}) &\leqslant \#G, \\ \#\mathrm{supp}(\psi) + \#\mathrm{supp}(\widehat{\psi}) &\leqslant \#G. \end{aligned}$$

Therefore, by Lemma 6.3, one has $\varphi = \psi = 0$.

This proves that the differential $D\Phi(f, g)$ is an isomorhism. □

Proof of Theorem 6.6. Since the map Φ in (6.4) is proper and dominant, the number of points in its fibers $\Phi^{-1}(w)$, counted with multiplicities is constant. See Fact 5.4. See also [18, Sec. 4].

Remembering Lemma 2.4 we want to prove that, counted with multiplicity, the number of points in the fiber $\Phi^{-1}(\mathbf{1}_{\mathbb{F}_p^*}, \mathbf{1}_{\mathbb{F}_p^*})$ is equal to $\binom{2n-2}{n-1}$.

It is equivalent to prove it for the fiber $\Phi^{-1}(\mathbf{1}_H, \mathbf{1}_H)$. This was done in the previous Lemma 6.8. □

Remark 6.9. It would be nice to have a similar counting formula for all $\mathcal{C}$-functions f on $\mathbb{F}_p$ with $f(1) = 1$.

7 Examples

From the previous sections one might get the feeling that there are "many" new unimodular $\mathcal{C}$-functions. We report in this chapter a few examples, relying on numerical experiments, that emphasize on the one hand the arithmetic complexity of these new unimodular $\mathcal{C}$-functions that we have proven to exist in this article, and on the other hand some kind of "uniqueness" of these new unimodular $\mathcal{C}$-functions if one takes into account the Galois action.

Remark 7.1. Before giving the examples it is important to notice the following fact. When f is a normalized odd $\mathcal{C}$-function on $\mathbb{Z}/d\mathbb{Z}$, and $a \in (\mathbb{Z}/d\mathbb{Z})^*$, the function $k \mapsto f(ak)/f(a)$ is also a normalized odd $\mathcal{C}$-function.

7.1 When $d = 7$

There are exactly $\binom{4}{2} = 6 = 1 \times 4 + 2$ odd $\mathcal{C}$-functions with $f(1) = 1$ on $\mathbb{F}_7$ counted with mutiplicities. All of them being Dirichlet characters. All of them except the Legendre character χ_0 having multiplicity 1.

All of them are unimodular $\mathcal{C}$-functions. As expected, this number is greater than $2^2 = 4$ which is the lower bound predicted by Theorem 2.3.

7.2 When $d = 9$

There are exactly 18 odd $\mathcal{C}$-functions with $f(1) = 1$ on the cyclic group $\mathbb{Z}/9\mathbb{Z}$. All of them having multiplicity one. Among those functions, there are no Dirichlet characters. These 18 functions are Galois conjugate.

The total number of unimodular odd $\mathcal{C}$-functions is 12. As expected, this number is greater than $2^3 = 8$ which is the lower bound predicted by Theorem 2.3.

These 12 odd unimodular $\mathcal{C}$-functions f are Galois conjugate. They are uniquely determined by the value $x = f(2)$. This value x is a unit of degree 18 over $\mathbb{Q}$. The minimal polynomial $R(T)$ of $t := x + x^{-1}$ over $\mathbb{Q}$ is

$$R(T) = T^9 - 36\,T^7 + 60\,T^6 + 144\,T^5 - 288\,T^4 - 96\,T^3 + 288\,T^2 - 64.$$

The value t must be chosen among the 6 real roots of $R(T)$ that belong to the interval $[-2, 2]$ so that x has absolute value equal to 1.

This field is $\mathbb{Q}[x] = \mathbb{Q}[c, u]$ where $c = \cos(2\pi/9)$ and where u has minimal polynomial over $\mathbb{Q}$

$$u^6 - 3u^4 - 105u^2 - 1.$$

We point out that this field $\mathbb{Q}[c]$ is an abelian extension of $\mathbb{Q}$ of degree 3 while the Galois closure of $\mathbb{Q}[u]$ has degree 24 and a solvable Galois group isomorphic to S_4. We denote by σ the Galois automorphism of $\mathbb{Q}[x]$ of order 3 given by

$$\sigma(c) = \cos(8\pi/9) \text{ and } \sigma(u) = u.$$

As in Remark (7.1), one can check that

$$\sigma(f(k)) = f(2k)/f(2), \text{ for all } k \in \mathbb{Z}/9\mathbb{Z}.$$

One has then

$$f = (0, 1, x, y, -\frac{1}{x''}, \frac{1}{x''}, -y, -x, -1)$$

where $x'' := \sigma^2(x)$ is also a root of $R(x'' + \frac{1}{x''}) = 0$, where $s := y + y^{-1}$ is a root of the polynomial

$$R_0(S) = 3S^9 + 18S^8 - 126S^6 - 108S^5 + 216S^4 + 252S^3 - 48S - 8,$$

and $\sigma(y) = -y/x$.

7.3 When $d = 11$

There are exactly $\binom{8}{4} = 70 = 1{\times}16 + 4 + 5 + 5 + 40$ odd $\mathcal{C}$-functions with $f(1) = 1$ on $\mathbb{F}_{11}$, counted with multiplicities. All of them except one having multiplicity one. The exception is the Legendre character χ_0 which has multiplicity 16. Among those functions, there are also the 4 Dirichlet characters of order 10. There are also the 5 real-valued (non-normalized) functions which are Galois conjugate to the function $k \mapsto (\frac{k}{11})\,(c(k^2) + 2\,c(4k^2))$ where $(\frac{k}{11})$ is the Legendre symbol and where $c(m) := \cos(2m\pi/11)$. There are also the 5 inverses of these functions.

The last 40 functions are Galois conjugate.

The total number of unimodular odd $\mathcal{C}$-functions, counted with multiplicities, is $30 = 1{\times}16 + 4 + 0 + 0 + 10$. As expected, this number 30 is greater than $2^4 = 16$ which is the lower bound predicted by Theorem 2.3.

We will describe more precisely these 10 new odd unimodular $\mathcal{C}$-functions since they are the simplest examples of Theorem 1.2. We will give explicit

Formulas for these functions as (7.1), (7.2) and (7.3). More importantly we will explain were these formulas come from.

The key point is that these new odd unimodular $\mathcal{C}$-functions f are Galois conjugate, and that they are uniquely determined by the value $x = f(2)$. This value x is a unit of degree 40 over $\mathbb{Q}$. One can explicitly compute the minimal polynomial $R(T)$ of $t := x + x^{-1}$ over $\mathbb{Q}$. It is given by

$$\begin{aligned} R(T) = {} & T^{20} - 17\,T^{19} + 31\,T^{18} + 562\,T^{17} - 1688\,T^{16} - 7001\,T^{15} + 27277\,T^{14} + 33355\,T^{13} \\ & - 204170\,T^{12} - 9265\,T^{11} + 811745\,T^{10} - 460189\,T^9 - 1890997\,T^8 + 1827614\,T^7 + 2787506\,T^6 \\ & - 3522554\,T^5 - 2493350\,T^4 + 3732202\,T^3 + 773431\,T^2 - 1642535\,T + 312643. \end{aligned}$$

The value t must be chosen among the 5 real roots of $R(T)$ that belong to the interval $[-2, 2]$ so that x has absolute value equal to 1. We fix such a root x of $R(x+\frac{1}{x}) = 0$ with $|x| = 1$ and we now describe the corresponding odd unimodular $\mathcal{C}$-function f.

The field $\mathbb{Q}[x]$ generated by x contains all the values $f(k)$. This field is $\mathbb{Q}[x] = \mathbb{Q}[c, u]$ where $c = \cos(2\pi/11)$ and u is a root of the irreducible polynomial over $\mathbb{Q}$

$$u^8 + 2u^7 - 2u^6 - 3u^5 + 3u^4 - 3u^3 - 2u^2 + 2u + 1.$$

We point out that this field $\mathbb{Q}[c]$ is an abelian extension of $\mathbb{Q}$ of degree 5 while the Galois closure of $\mathbb{Q}[u]$, which is $\mathbb{Q}[u, \sqrt[3]{11}, i\sqrt{3}]$, has degree 48 and has a solvable Galois group isomorphic to $\mathrm{GL}(2, \mathbb{F}_3)$. We denote by σ the Galois automorphism of $\mathbb{Q}[x]$ of order 5 given by

$$\sigma(c) = \cos(8\pi/11) \ \text{ and } \ \sigma(u) = u.$$

As in Remark (7.1), one can check that

$$\sigma(f(k)) = f(2k)/f(2), \text{ for all } k \in \mathbb{F}_{11}.$$

We introduce the five roots of $R(x+\frac{1}{x}) = 0$ given by

$$x_m := \sigma^{m-1}(x) \ \text{ for } \ m = 1, \ldots 5,$$

so that $f(2^m) = x_1 \cdots x_m$. Since σ commutes with the complex conjugation, all of them have absolute value $|x_m| = 1$. One has

$$x_1 x_2 x_3 x_4 x_5 = -1 \ \text{ and}$$

$$f = (0, 1, x_1, \tfrac{1}{x_4 x_5}, x_1 x_2, \tfrac{-1}{x_5}, \tfrac{1}{x_5}, -x_1 x_2, \tfrac{-1}{x_4 x_5}, -x_1, -1). \tag{7.1}$$

One can describe even more explicitly these roots x_m. Let us label the five real roots t_m of the polynomial $R(T)$ in the interval $[-2, 2]$ as

$$t_1 < t_3 < t_5 < t_2 < t_4. \tag{7.2}$$

These labels might look surprising. They are adapted to the Galois action: if we choose x to be $x = t_1 + i\sqrt{4 - t_1^2}$ then one has

$$x_m = t_m + i\sqrt{4 - t_m^2} \text{ for } 1 \leqslant m \leqslant 4 \text{ and } x_5 = t_5 - i\sqrt{4 - t_5^2}. \tag{7.3}$$

The ten new normalized unimodular $\mathcal{C}$ function are the functions obtained from the function f given in (7.1) by circular permutation on the indices $m \in \mathbb{Z}/5\mathbb{Z}$, and their complex conjugates.

7.4 When $d = 13$

There are exactly $\binom{10}{5} = 252 = 2 + 4 + 6 + 96 + 144$ odd $\mathcal{C}$-functions with $f(1) = 1$ on $\mathbb{F}_{13}$ all of them with multiplicity 1. Among those, are the 2 Dirichlet characters of order 4 and the 4 Dirichlet characters of order 12. Among those are also 6 other odd functions f such that, for some $\varepsilon = \pm 1$, one has

$$f(5x) = i^{\varepsilon} f(x) \text{ for all } x. \tag{7.4}$$

The remaining functions form two Galois conjugacy classes, the first one contains 96 functions, the last one contains 144 functions.

The total number of unimodular odd $\mathcal{C}$-functions is $60 = 2+4+6+0+48$. As expected, this number 60 is greater than $2^5 = 32$ which is the lower bound predicted by Theorem 2.3.

It follows from this discussion that beyond the 6 new unimodular $\mathcal{C}$-functions satisfying (7.4) the 48 other new unimodular $\mathcal{C}$-functions are Galois conjugate. These functions happen to be uniquely determined by the value $x = f(2)$ which is a unit of degree 144 over $\mathbb{Q}$. One can explicitely compute the minimal polynomial $R(T)$ of $t := x + x^{-1}$ over $\mathbb{Q}$. It is given by

$$R(T) = T^{72} - 26\,T^{71} - 254\,T^{70} + 10604\,T^{69} + 7528\,T^{68} - 1791202\,T^{67} + 3759135\,T^{66} + \ldots$$
$$+ \ldots - 290452953005519364096\,T + 3553050924129292288$$

The value t must be chosen among the 24 real roots of $R(T)$ that belong to the interval $[-2, 2]$ so that x has absolute value equal to 1.

The construction of f from x can then be obtained following a similar pattern as when $d = 11$.

A Appendix: Biunimodular functions

Harvey Cohn's problem was developped simultaneously with the very popular problem which is called the *biunimodular functions problem* and is due to Per Enflo. The aim of this appendix is to recall part of the history of this problem and to explain in Theorem A.1 new constructions of biunimodular functions that can be obtained by the method we have developped in this paper.

A.1 Classical biunimodular functions

Let d be an integer.

Definition. A complex valued function f on the cyclic group $C_d := \mathbb{Z}/d\mathbb{Z}$ is called *unimodular* if $|f(\ell)| = 1$ for all $\ell \in C_d$.

This definition is different from the definition in Section 1.1 since the function f does not vanish at 0.

Definition. A unimodular function f is called *biunimodular* if its Fourier transform $\widehat{f}$ is also unimodular.

It is equivalent to require

$$\sum_{k\in\mathbb{Z}/d\mathbb{Z}} f(k-\ell)\overline{f(k)} \;=\; 0 \quad \text{for all } \ell \neq 0. \tag{A.1}$$

Geometrically, Condition (A.1) means that the translates of f form an orthogonal basis of $\ell^2(C_d)$.

This notion was introduced by Per Enflo in the 80's in relation with the "circulant complex Hadamard matrices". The simplest examples of biunimodular functions are the gaussian functions. We recall that, when d is odd, a gaussian function on the cyclic group $C_d = \mathbb{Z}/d\mathbb{Z}$ is a function of the form

$$g_{m,a} : x \mapsto e^{2i\pi m(x-a)^2/d} \tag{A.2}$$

for some m, a in $\mathbb{Z}/d\mathbb{Z}$, m coprime to d.

Per Enflo asked for the existence of other biunimodular functions, when $d = p > 2$ is prime. Björck answered in 1989 by classifying in [9] the biunimodular functions that are $(\mathbb{F}_p^*)^2$-invariant. These functions were also independently discovered and used by de la Harpe with Jones in [14] and by Munemasa with Watatani in [28]. They found:

When $p \equiv 1 \bmod 4$ there are, up to proportionality, four such functions

$$h_\varepsilon = \delta_0 + \cos\theta\, \mathbf{1}_{\mathbb{F}_p^*} + i\,\varepsilon_2 \sin\theta\, \chi_0,$$

where χ_0 is the Legendre character, $\cos\theta := \frac{1}{\varepsilon_1\sqrt{p}+1}$ and $\varepsilon_1, \varepsilon_2 = \pm 1$.

When $p \equiv 3 \bmod 4$ there are, up to proportionality, four such functions

$$h_\varepsilon = e^{i\,\theta}\delta_0 + cos\theta\, \mathbf{1}_{\mathbb{F}_p^*} + i\,\varepsilon_2 \sin\theta\, \chi_0,$$

where χ_0 is the Legendre character, $\tan\theta = \varepsilon_1\sqrt{p}$ and $\varepsilon_1, \varepsilon_2 = \pm 1$.

We introduce the slight variations $h_{\varepsilon,a,b}$ of these functions, where $a, b \in \mathbb{F}_p$,

$$h_{\varepsilon,a,b} : x \mapsto e^{2i\pi ax/p}\, h_\varepsilon(x-b). \tag{A.3}$$

For all prime $p \geqslant 7$, this gives rise to $4p^2$ new biunimodular functions that we call the Björck functions.

Haagerup proved in 2008 in [18] that, when p is prime, the set of biunimodular functions with $f(0) = 1$ is finite.

When $p \equiv 1 \bmod 3$ is prime, biunimodular functions on $\mathbb{F}_p$ which are $(\mathbb{F}_p^*)^3$-invariant have been classified by Gabidulin and Shorin in [17] and by Björck and Haagerup in [10]. This gave rise to new biunimodular functions for all prime $p \equiv 1 \bmod 3$, $p \geqslant 13$. Their method relies on explicit computations that are possible since the $(\mathbb{F}_p^*)^3$-invariant functions f with $f(0) = 1$ depend only on three parameters.

Using the same strategy when $p \equiv 1 \bmod 5$, a few computer assisted constructions of $(\mathbb{F}_p^*)^5$-invariant biunimodular functions were given for a few values of p in [26]: $p = 31$ and $p = 61$.

Biunimodular functions are studied under various names like CAZAC, PSK perfect sequences, polyphase sequences with optimum correlation and so on. See [3], [15], [16] and [29] for strongly related topics.

A.2 Constructing biunimodular functions

The method we developped in this paper allows us to have a new insight in the Enflo problem. For instance we will prove:

Theorem A.1. *Let $p \geqslant 11$ be prime. There exist biunimodular functions on $\mathbb{F}_p$ which are proportional neither to gaussian nor to Björck functions.*

The proof will be similar to the proof of Theorem 1.2. Let $V := \ell^2(\mathbb{F}_p)$ be the p-dimensional Hilbert space of functions f on $\mathbb{F}_p$. Let $\mathbb{P}(V) \simeq \mathbb{CP}^{p-1}$ be the projective space of V, let T be the Clifford torus

$$T := \{[f] \in \mathbb{P}(V) \mid \ |f(x)| = |f(0)| \text{ for all } x \in \mathbb{F}_p\} \simeq \mathbb{T}^{p-1}. \tag{A.4}$$

and $F : f \mapsto \widehat{f}$ be the Fourier transform given by (2.1).

Proof of Theorem A.1. We will apply Theorem 2.3 to the unitary transformation F and the torus T. The $(p-1)p$ gaussian functions $g_{m,a}$ as in (A.2) belong to the intersection $T \cap F^{-1}T$. The $4p^2$ functions $h_{\varepsilon,a,b}$ as in (A.3) also belong to the intersection $T \cap F^{-1}T$.

Assume, by contradiction that the intersection $T \cap F^{-1}T$ contains only gaussian and Björck functions. Then, by the following Propositions A.2 and A.3, this intersection is transverse. Therefore Theorem 2.3 predicts the existence of at least 2^{p-1} intersection points counted with multiplicity. Since $p \geqslant 11$, one has $2^{p-1} > (p-1)p + 4p^2$, there must exist another intersection point. This is the contradiction we are looking for. □

The proof relied on transversality properties that will be proven in Sections A.3 and A.4.

A.3 Transversality at gaussian functions

Let $p \geqslant 3$ be prime. The aim of this section is to prove the transversality of the intersection $T \cap F^{-1}T$ at the gaussian functions. To simplify notation we will only deal with one gaussian function.

Proposition A.2. *Let $p \geqslant 3$ be prime and g_0 be the gaussian function on $\mathbb{F}_p$, $x \mapsto g_0(x) := e^{2i\pi x^2/p}$. Then the intersection $T \cap F^{-1}T$ is transverse at $[g_0]$.*

Proof of Proposition A.2. We compute the Fourier transform: for x in $\mathbb{F}_p$,

$$\widehat{g}_0(x) \ = \ \varepsilon_p \, \overline{g_0}(x/2),$$

where $\varepsilon_p := \frac{G(\chi_0)}{\sqrt{p}}$ and where $1/2$ is the inverse of 2 in $\mathbb{F}_p$.

Note that $\varepsilon_p = 1$ when $p \equiv 1 \bmod 4$ and $\varepsilon_p = i$ when $p \equiv 3 \bmod 4$.

$\star$ **We describe the tangent space to the projective space.**
It will be convenient to use a parametrization of a neighborhood of $[g_0]$ in $\mathbb{P}(V)$ by the vector space $V_o := \{\varphi \in \mathbb{C}^{\mathbb{F}_p} \mid \varphi(0) = 0\}$ given by

$$\varphi \mapsto [g_\varphi] \text{ where } g_\varphi = \left(\mathbf{1}_{\mathbb{F}_p} + \varphi\right) g_0 .$$

This gives an identification of V_o with the tangent space of $\mathbb{P}(V)$ at the point $[g_0]$, thanks to the formula

$$\varphi \mapsto v_\varphi := \frac{d}{d\varepsilon}[g_{\varepsilon\varphi}]|_{\varepsilon=0} \in T_{[g_0]}\mathbb{P}(V).$$

$\star$ **We describe the tangent space to the torus** T. Since $\varphi(0) = 0$, the linear condition defining the tangent space of T at the point $[g_0]$ is

$$\mathrm{Re}(\varphi) = 0. \tag{A.5}$$

$\star$ **We describe the tangent space to the torus** $F^{-1}T$. One computes in our coordinate system

$$\begin{aligned} \widehat{g}_\varphi &= \left(\mathbf{1}_{\mathbb{F}_p} + U\varphi\right) \widehat{g}_0 \text{ where} \\ U\varphi(x) &= \varepsilon_p^{-1}\, g_0(x/2) \textstyle\sum_{y\in\mathbb{F}_p} e^{2i\pi xy/p} e^{2i\pi y^2/p} \varphi(y) \\ &= \varepsilon_p^{-1} \textstyle\sum_{y\in\mathbb{F}_p} g_0(x/2+y)\, \varphi(y) \\ &= \varepsilon_p^{-1}\, (g_0 * \varphi)(-x/2), \text{ for all } x \text{ in } \mathbb{F}_p. \end{aligned}$$

The linear condition defining the tangent space of $F^{-1}T$ at the point $[g_0]$ is

$$\mathrm{Re}(U\varphi) \text{ is constant on } \mathbb{F}_p. \tag{A.6}$$

$\star$ **We check the transversality of these tangent spaces**. We want to prove that a function $\varphi \in V_o$ belonging to both tangent spaces is zero. By (A.5) one can write $\varphi = i\psi$ with ψ real valued. We set $g_0 = \alpha_0 + i\beta_0$ where

$$\alpha_0(x) = \cos(2\pi x^2/p) \text{ and } \beta_0(x) := \sin(2\pi x^2/p).$$

and we distinguish two cases.

First case: when $p \equiv 1$ **mod** 4. Equation (A.6) can be rewritten as

$$\beta_0 * \psi \text{ is constant on } \mathbb{F}_p.$$

or equivalently

$$\widehat{\beta}_0\widehat{\psi} \text{ is zero on } \mathbb{F}_p^*.$$

Since the function $\widehat{\beta}_0(x) = -\beta_0(x/2)$ does not vanish on $\mathbb{F}_p^*$, this implies that $\widehat{\psi}$ is zero on $\mathbb{F}_p^*$. Therefore, since $\sum_y \widehat{\psi}(y) = \sqrt{p}\,\psi(0) = 0$, one gets $\widehat{\psi} = 0$ and $\psi = 0$, as required.

Second case: when $p \equiv 3$ mod 4. Equation (A.6) can be rewritten as

$$\alpha_0 * \psi \text{ is constant on } \mathbb{F}_p.$$

or equivalently

$$\widehat{\alpha}_0\widehat{\psi} \text{ is zero on } \mathbb{F}_p^*.$$

Since the function $\widehat{\alpha}_0(x) = i\,\alpha_0(x/2)$ does not vanish on $\mathbb{F}_p^*$, this implies that $\widehat{\psi}$ is zero on $\mathbb{F}_p^*$. Therefore, as above, the function ψ is 0. □

A.4 Transversality at Björck functions

Let $p \geqslant 3$ be prime. The aim of this section is to prove the transversality of the intersection $T \cap F^{-1}T$ at the Björck functions. To simplify we will only deal with one such function and choose notation that works both for $p \equiv \pm 1$ mod 4.

When $p \equiv 1$ mod 4, we set $\theta_0 = 0$ and $\theta = \arccos(\frac{1}{\sqrt{p}+1})$.

When $p \equiv 3$ mod 4, we set $\theta_0 = \theta = \arctan(\sqrt{p})$.

Proposition A.3. *Let h_0 be the Björck function on $\mathbb{F}_p$,*

$$h_0 \;=\; e^{i\,\theta_0}\delta_0 + \cos\theta\,\mathbf{1}_{\mathbb{F}_p^*} + i\sin\theta\,\chi_0. \tag{A.7}$$

Then the intersection $T \cap F^{-1}T$ is transverse at $[h_0]$.

Proof of Proposition A.3. We compute the Fourier transform:

$$\varepsilon_p^{-1}\,\widehat{h}_0 \;=\; e^{-i\,\theta_0}\delta_0 + \cos\theta\,\mathbf{1}_{\mathbb{F}_p^*} + i\sin\theta\,\chi_0, \tag{A.8}$$

where $\varepsilon_p = 1$ when $p \equiv 1$ mod 4 and $\varepsilon_p = i$ when $p \equiv 3$ mod 4.

⋆ **We describe the tangent space to the projective space.** The set B of Dirichlet characters on $\mathbb{F}_p$ is a basis of V_o. It will be convenient to use

the following coordinates system $\mathbf{a} = (\mathbf{a}_\chi)_{\chi\in B}$ of $\mathbb{P}(V)$ in the neighborhood of $[h_0]$ where the coordinates $\mathbf{a}_\chi$ are complex numbers. It is given by

$$\mathbf{a} \mapsto [h_{\mathbf{a}}] \text{ where } h_{\mathbf{a}} = \left(\mathbf{1}_{\mathbb{F}_p} + \sum_{\chi\in B} \mathbf{a}_\chi \chi\right) h_0 \,.$$

These coordinates $\mathbf{a} = (\mathbf{a}_\chi) \in \mathbb{C}^B$ are also a linear coordinate system for the tangent space of $\mathbb{P}(V)$ at the point $[h_0]$, thanks to the formula

$$\mathbf{a} \mapsto v_{\mathbf{a}} := \frac{d}{d\varepsilon}[h_{\varepsilon\mathbf{a}}]|_{\varepsilon=0} \ \in \ T_{[h_0]}\mathbb{P}(V).$$

⋆ **We describe the tangent space to the torus** T. Since the characters χ vanish at 0, the linear condition defining the tangent space of T at the point $[h_0]$ is

$$\mathrm{Re}(\textstyle\sum_{\chi\in B} \mathbf{a}_\chi \chi) \ = \ 0.$$

By the linear independance of the characters, this can be rewritten as

$$\overline{\mathbf{a}_{\overline{\chi}}} = -\mathbf{a}_\chi \text{ for all } \chi \in B. \tag{A.9}$$

⋆ **We describe the tangent space to the torus** $F^{-1}T$. Using (3.5), one computes in our coordinate system

$$\begin{aligned}
h_{\mathbf{a}} &= h_0 + \textstyle\sum_{\chi\in B}(\cos\theta\, \mathbf{a}_\chi + i\, \sin\theta\, \mathbf{a}_{\chi_0\chi})\chi \,, \\
\widehat{h}_{\mathbf{a}} &= \left(\mathbf{1}_{\mathbb{F}_p} + \mathbf{b}_0\, \delta_0 + \textstyle\sum_{\chi\in B} \mathbf{b}_\chi \overline{\chi}\right) \widehat{h}_0 \quad \text{where} \\
\mathbf{b}_0 &= \tfrac{p-1}{\varepsilon_p\sqrt{p}}\,(\cos\theta\, \mathbf{a}_{\mathbf{1}} + i\, \sin\theta\, \mathbf{a}_{\chi_0})\, e^{i\theta_0}, \\
\textstyle\sum_{\chi\in B} \mathbf{b}_\chi\overline{\chi} &= \displaystyle\sum_{\chi\in B} \tfrac{G(\chi)}{\varepsilon_p\sqrt{p}}(\cos\theta\, \mathbf{a}_\chi + i\, \sin\theta\, \mathbf{a}_{\chi_0\chi})(\cos\theta\, \overline{\chi} - i\, \sin\theta\, \chi_0\overline{\chi}),
\end{aligned}$$

where $G(\chi)$ is the Gauss sum (3.3). The extra term $\mathbf{b}_0\, \delta_0$ comes from the extra term in (3.5) when $\chi = \mathbf{1}_{\mathbb{F}_p^*}$ is the trivial Dirichlet character. The coefficients $\mathbf{b}_\chi$ are then given by

$$\mathbf{b}_\chi = \tfrac{G(\chi)\cos\theta^2 + G(\chi_0\chi)\sin\theta^2}{\varepsilon_p\sqrt{p}}\, \mathbf{a}_\chi + i\tfrac{(G(\chi) - G(\chi_0\chi))\cos\theta\, \sin\theta}{\varepsilon_p\sqrt{p}}\, \mathbf{a}_{\chi_0\chi} \tag{A.10}$$

In particular, for the trivial character, one has

$$\mathbf{b}_{\mathbf{1}} \ := \ \tfrac{-\cos\theta^2 + \varepsilon_p\sqrt{p}\, \sin\theta^2}{\varepsilon_p\sqrt{p}}\, \mathbf{a}_{\mathbf{1}} - i\, \tfrac{(1+\varepsilon_p\sqrt{p})\, \cos\theta\, \sin\theta}{\varepsilon_p\sqrt{p}}\, \mathbf{a}_{\chi_0}$$

As above, the linear condition defining the tangent space of $F^{-1}T$ at the point $[h_0]$ is

$$\begin{aligned} \overline{\mathbf{b}_{\overline{\chi}}} + \mathbf{b}_\chi &= 0\,, \text{ for all } \chi \in B \text{ non trivial, and} \\ \mathrm{Re}(\mathbf{b}_0 - \mathbf{b_1}) &= 0\,, \text{ for the trivial character } \chi = \mathbf{1}_{\mathbb{F}_p^*}. \end{aligned} \tag{A.11}$$

$\star$ **We check the transversality of these tangent spaces**. We want to prove that if $\mathbf{a} = (\mathbf{a}_\chi)_{\chi\in B}$ belongs to both tangent spaces, then $\mathbf{a} = 0$. By (A.9) one has $\overline{\mathbf{a}_{\overline{\chi}}} = -\mathbf{a}_\chi$ for all $\chi \in B$. One computes

$$\chi(-1)\overline{\mathbf{b}_{\overline{\chi}}} = -\frac{G(\chi)\cos\theta^2 + \chi_0(-1)G(\chi_0\chi)\sin\theta^2}{\varepsilon_p\sqrt{p}}\mathbf{a}_\chi + i\frac{(G(\chi) - \chi_0(-1)G(\chi_0\chi))\cos\theta\,\sin\theta}{\varepsilon_p\sqrt{p}}\mathbf{a}_{\chi_0\chi}. \tag{A.12}$$

In order to exploit (A.11), we distinguish two cases.

First case: when $p \equiv 1$ **mod** 4.
One has $\varepsilon_p = 1$, $\chi_0(-1) = 1$, $\theta_0 = 0$ and $\cos\theta = \frac{1}{\sqrt{p}+1}$.
• If χ is odd. One combines the equations (A.10), (A.11) and (A.12). One gets

$$(G(\chi)\cos\theta^2 + G(\chi_0\chi)\sin\theta^2)\,\mathbf{a}_\chi = 0.$$

Hence since $|G(\chi)| = |G(\chi_0\chi)|$, one concludes $\mathbf{a}_\chi = 0$.
• If χ is even and $\chi \neq \chi_0$. One combines the equations (A.10), (A.11) and (A.12) for the character $\chi_0\chi$. One gets

$$(G(\chi) - G(\chi_0\chi))\,\mathbf{a}_\chi = 0. \tag{A.13}$$

Hence by Lemma A.4, one concludes $\mathbf{a}_\chi = 0$.
• If $\chi = \chi_0$. Instead of (A.13), one writes $0 = \mathrm{Re}(\mathbf{b}_0 - \mathbf{b_1}) = i\sqrt{p}\,\sin\theta\,\mathbf{a}_{\chi_0}$. One concludes $\mathbf{a}_{\chi_0} = 0$.

Second case: when $p \equiv 3$ **mod** 4.
One has $\varepsilon_p = i$, $\chi_0(-1) = -1$, $\theta_0 = \theta$ and $\tan\theta = \sqrt{p}$.
• If χ is odd and $\chi \neq \chi_0$. One combines the equations (A.10), (A.11) and (A.12). One gets

$$G(\chi)\cos\theta\,\mathbf{a}_\chi - i\,G(\chi_0\chi)\sin\theta\,\mathbf{a}_{\chi_0\chi} = 0 \tag{A.14}$$

Applying the same calculation to the even character $\chi_0\chi$, one gets

$$i\,G(\chi_0\chi)\cos\theta\,\mathbf{a}_\chi + G(\chi)\sin\theta\,\mathbf{a}_{\chi_0\chi} = 0 \tag{A.15}$$

The determinant of this linar system is $D := (G(\chi)^2 - G(\chi_0\chi)^2)\cos\theta\sin\theta$. By Lemma A.4, this determinant is non zero. Therefore one has $\mathbf{a}_\chi = 0$.
• If $\chi = \chi_0$. Equation (A.14) is still valid and gives $\mathbf{a_1} + \mathbf{a}_{\chi_0} = 0$. Instead of (A.15), one writes $0 = \mathrm{Re}(\mathbf{b}_0 - \mathbf{b_1}) = -i\sqrt{p}\,\mathbf{a_1}$. Combining these two equalities, one concludes $\mathbf{a}_{\chi_0} = 0$.
• If χ is even. One applies the previous discussion to the odd character $\chi_0\chi$ and one also gets $\mathbf{a}_\chi = 0$. □

We have used the following

Lemma A.4. *Let p be a prime number, let χ_0 be the Dirichlet character on $\mathbb{F}_p$ of order 2 and let χ be another Dirichlet character on $\mathbb{F}_p$. Then the ratio of Gauss sums $R(\chi) := \dfrac{G(\chi_0\chi)}{G(\chi)}$ is not a root of unity.*

Proof. When $\chi = \chi_0$ or χ is trivial the ratio does not have absolute value 1. Otherwise, one has the equality $R(\chi) = \dfrac{G(\chi_0)}{J(\chi,\chi_0)}$ where J is the Jacobi sum (3.1). By Proposition 3.1, the ratio $\dfrac{\overline{R(\chi)}}{R(\chi)} = \pm\dfrac{J(\chi,\chi_0)}{J(\overline{\chi},\chi_0)}$ is not a root of unity. Therefore the ratio $R(\chi)$ is not a root of unity either. □

This ends the proof of Theorem A.1.

Declaration The author is a CNRS researcher, he has no relevant competing interest with this article and he has not used computer datas in the proofs.

References

[1] I. Aizenberg and A. Yuzhakov. *Integral representations and residues in multidimensional complex analysis*, volume 58 of *Transl. Math. Mon.* AMS, 1983.

[2] O. Andersson and I. Bengtsson. Clifford tori and unbiased vectors. *Rep. Math. Phys.*, 79:33–51, 2017.

[3] J. J. Benedetto, K. Cordwell, and M. Magsino. CAZAC sequences and Haagerup's characterization of cyclic N-roots. In *New trends in applied harmonic analysis*, pages 1–43. Birkhäuser, 2019.

[4] Y. Benoist. Convolution and square in abelian groups I. *Experimental Mathematics,* 33:518-528 , 2023.

[5] Y. Benoist. Convolution and square in abelian groups II. hal-03744506 (2022) and *Journal de Théorie des nombres de Bordeaux,* (to appear) 60 p.

[6] P. Biran, M. Entov, and L. Polterovich. Calabi quasimorphisms for the symplectic ball. *Commun. Contemp. Math.*, 6:793–802, 2004.

[7] A. Biró. Notes on a problem of H. Cohn. *J. Number Theory*, 77:200–208, 1999.

[8] A. Biró and V. F. Lev. Uncertainty in finite planes. *J. Funct. Anal.*, 281:Paper No. 109026, 32, 2021.

[9] G. Björck. Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and "cyclic n-roots". In *Recent advances in Fourier analysis and its applications*, pages 131–140. 1990.

[10] G. Björck and U. Haagerup. All cyclic p-roots of index 3, found by symmetry-preserving calculations. arXiv:0803.2506.

[11] P. Borwein, K.-K. S. Choi, and S. Yazdani. An extremal property of Fekete polynomials. *Proc. Amer. Math. Soc.*, 129:19–27, 2001.

[12] C.-H. Cho. Holomorphic discs, spin structures, and Floer cohomology of the Clifford torus. *Int. Math. Res. Not.*, 35:1803–1843, 2004.

[13] K.-K. Choi and M.-K. Siu. Counter-examples to a problem of Cohn on classifying characters. *J. Number Theory*, 84:40–48, 2000.

[14] P. de la Harpe and V. Jones. Paires de sous-algèbres semi-simples et graphes fortement réguliers. *C. R. Acad. Sci.*, 311:147–150, 1990.

[15] J.-C. Faugère. Finding all the solutions of Cyclic 9 using Gröbner basis techniques. In *Computer mathematics*, LN Ser. Comput., pages 1–12. 2001.

[16] H. Führ and Z. Rzeszotnik. On biunimodular vectors for unitary matrices. *Linear Algebra Appl.*, 484:86–129, 2015.

[17] E. M. Gabidulin and V. V. Shorin. New sequences with zero autocorrelation. *Problemy Peredachi Informatsii*, 38:10–23, 2002.

[18] U. Haagerup. Cyclic p-roots of prime lengths p and related complex Hadamard matrices. arXiv:0803.2629.

[19] H. Halberstam and H.-E. Richert. *Sieve methods.* Academic Press, 1974.

[20] M. Idel and M. Wolf. Sinkhorn normal form for unitary matrices. *Linear Algebra Appl.*, 471:76–84, 2015.

[21] K. Ireland and M. Rosen. *A classical introduction to modern number theory.* GTM 84. Springer, 1990.

[22] H.-J. Kanold. Über eine zahlentheoretische Funktion von Jacobsthal. *Math. Ann.*, 170:314–326, 1967.

[23] O. Klurman and A. P. Mangerel. Rigidity theorems for multiplicative functions. *Math. Ann.*, 372:651–697, 2018.

[24] P. Kurlberg. On a character sum problem of Cohn. *J. Number Theory*, 92:174–181, 2002.

[25] S. Lang. *Cyclotomic fields I and II.* GTM 121. Springer, 1990.

[26] P. Loidreau and V. Shorin. Application of Groebner bases for searching new sequences with good periodic correlation properties. 2005 IEEE ISIT.

[27] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis.* CBMS 84. AMS, 1994.

[28] A. Munemasa and Y. Watatani. Paires orthogonales de sous-algèbres involutives. *C. R. Acad. Sci.*, 314:329–331, 1992.

[29] R. Nicoarùa. A finiteness result for commuting squares of matrix algebras. *J. Operator Theory*, 55:295–310, 2006.

[30] L. Smith. *Polynomial invariants of finite groups.* Peters, 1995.

[31] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18:26–37, 1996.

[32] T. Tao. An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett.*, 12:121–127, 2005.

[33] A. Terras. *Fourier analysis on finite groups and applications.* London Math. Soc. Stud. Texts 43. CUP, 1999.

[34] A. Tsikh. *Multidimensional residues and their applications.* Transl. Math. Mon. AMS, 1992.

Y. Benoist: CNRS, Université Paris-Saclay, yves.benoist@cnrs.fr