The Equiangular Dream

Yves Benoist

Lectures at Orsay, February-May 2025
Preliminary draft

Abstract

Equiangular configurations of lines are geometric objects that were first discovered in Quantum Computer Science in the late 1990's. Understanding the construction of these equiangular lines is still an open problem.

The aim of this graduate course is to introduce the mathematical tools that allow us to better understand this problem and to deal with other similar problems.

The basic tool is the Fourier transform on finite abelian groups. This basic tool will be combined with more advanced mathematical tools like Floer homology, theta functions, elliptic curves, modular forms, ray class fields...

No need to know these advanced topics to read this course. The point of view will be to give a comprehensive introduction and to use them as black boxes. We will understand why these advanced topics are useful for concrete questions instead of learning them in depth.

Contents

Introduction

The aim of this graduate course is not to present a classical mathematical theory as the semisimple Lie groups, the algebraic curves, the random walks, the class field theory or the potential theory.

Instead we will present a few concrete problems whose statement looks naive but are still partially conjectural. Eventhough these statements are less accessible than what one could foresee at first glance, they give rise to nice partial results whose proof will force us to learn useful mathematical tools.

The aim of this course is to emphasize this lively and experimental aspects of mathematics, and simultaneously, to emphasize the fact that the classical mathematical theories happen often to be useful for solving concrete problems.

The concrete problems discussed in this course are related to the cyclic group $\mathbb{Z}/d\mathbb{Z}$ and can easily be checked for small values of the integer d. But already for values like $d = 11$ they seem to be accessible only thanks to these theorical tools.

More precisely we will successively discuss the following three elementary problems of linear algebra. They take place in the d-dimensional hermitian vector space $\mathbb{C}^d$. It will be convenient to identify this vector space $\mathbb{C}^d$ with the space $\mathbb{C}[\mathbb{Z}/d\mathbb{Z}]$ of complex valued functions f on the cyclic group $\mathbb{Z}/d\mathbb{Z}$.

Problem 1: Describe the biunimodular functions

These are functions f on $\mathbb{Z}/d\mathbb{Z}$ with constant modulus equal to 1 and whose Fourier transform also has constant modulus equal to 1. This can be written as $|f| = |\widehat{f}| = 1$. Equivalently f is a function with constant modulus equal to 1 which is orthogonal to its translates. Up to a scalar, there are only finitely many biunimodular functions when d is prime. This problem finds its roots in the theory of signal in the 80's. It is also known in computer science under the name "Cyclic d-roots" and in operator algebra under the name "Circulant complex Hadamard matrix".

Problem 2: Find critical functions.

These are non zero functions on $\mathbb{Z}/d\mathbb{Z}$ with d odd whose convolution square is proportional to their square. More precisely, we want the function f to satisfy $f*f(2\ell) = \lambda f^2(\ell)$. The proportionality constant λ is called a critical value. There are only finitely many critical values. This problem is related to theta functions.

Problem 3: Construct d^2 equiangular lines in $\mathbb{C}^d$.
This number d^2 is an upper bound of the number of lines in $\mathbb{C}^d$ for which the angles between two of them is constant. We will try to construct these d^2 lines $\mathbb{C}f_{j,k}$ in $\mathbb{C}[\mathbb{Z}/d\mathbb{Z}]$ indexed by pairs $(j,k) \in (\mathbb{Z}/d\mathbb{Z})^2$ and given by the formula $f_{j,k}(\ell) = e^{2i\pi j\ell/d} f(\ell + k)$ where f is a function one needs to find. Up to a unitary transformation of $\mathbb{C}^d$, there should be only finitely many such configurations, when $d \geqslant 4$. This problem finds its roots in quantum computer science in the 90's where it is known under the acronym "Sicpovm". This part of the course will contain very few proved results. We will instead present what the experts expect. We will call it the equiangular dream.

These three problems are independent of one another but the analogy between them is striking because they have many common features.
- Complex algebraic geometry plays an important role.
- The Galois group of $\mathbb{Q}$ and the p-adic fields too.
- When a function f is solution, the functions $f_{j,k}$ are also solutions.
- When a function f is solution, its Fourier tansform $\widehat{f}$ too.
- These problems can be numerically tested for d small.
- The complexity grows quickly with d.
- The known answers are only partial and uses unexpected tools.

These three problems have their own specificity and need black boxes.
- The first one needs symplectic geometry.
- The second one needs abelian varieties.
- The last one needs class field theory.

Part I

Biunimodular functions

The first three lectures will deal with the Fourier transform on cyclic groups, often focusing on the case where the cyclic group $G = C_d$ has prime order $d = p$ which is particularly interesting.

In the first lecture we will check an uncertainty principle due to Cebotarev. The main tool is the estimation of the p-adic valuation of certain determinants.

In the second lecture we will introduce a family of functions on G called biunimodular, that have properties analogous to the gaussian functions. They have constant modulus and their Fourier transform too. We will check that the number of such functions up to scalar is finite, and we will give a precise upper bound on this number. The main tools come from complex algebraic geometry.

In the third lecture we will explain how to construct new biunimodular functions by using intersection properties of Clifford tori in the complex projective space. These properties rely on Floer homology.

In this third lecture we will also introduce a family of functions on G called biunimodular on $C_d \smallsetminus \{0\}$. They are functions that vanishes at 0 and have constant modulus outside 0 and their Fourier transform too. When $d = p$ is prime, they have properties analogous to the Dirichlet characters. We will focus particularly on the case of odd-biunimodular functions.

By the same methods as above, we will check that the number of such functions up to scalar is finite, and we will give a precise upper bound on this number. We will also construct new odd-biunimodular functions. In this case a useful tool is an estimation of the p-adic valuation of Jacobi sums due to Kummer and Stickelberger.

1 Finite Fourier transform

The first lecture deals with the finite Fourier transform.

We first study the quadratic Gauss sums, their relation with the Jacobi symbols, and with the multiplicity of the eigenvalues of the Fourier transform on the cyclic group $\mathbb{Z}/d\mathbb{Z}$.

Using Dirichlet characters, we then study the properties of the general Gauss sums together with the Jacobi sums.

We end this lecture by proving the uncertainty principle for the finite Fourier transform on a cyclic group of prime order.

1.1 Definition and properties

Let G be a finite abelian group of order d. The vector space $\mathbb{C}[G]$ of complex valued functions on G is a hermitian vector space for the hermitian form $\|f\|^2_{\ell^2} = \sum_{j\in G} |f(j)|^2$. The Dirac functions $(\delta_j)_{j\in G}$ form an orthonormal basis of $\mathbb{C}[G]$. This identifies the space $\mathbb{C}[G]$ with the standard hermitian vector space $\mathbb{C}^d$.

An important example is the cyclic group $G = C_d = \mathbb{Z}/d\mathbb{Z}$ which is also a ring. When $d = p$ is prime, we will use the notation $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. This ring is then a field.

We first recall the definition of the finite Fourier transform on G Let $\widehat{G} = \mathrm{Hom}(G, \mathbb{Z}/d\mathbb{Z})$ the dual abelian group. For j in $\widehat{G}$ and k in G, it will be nice to denote by jk the element $j(k) \in \mathbb{Z}/d\mathbb{Z}$. This notation is convenient because, when $G = C_d$, the dual group has a natural identification with C_d so that jk is nothing but the product of j and k in the ring C_d.

We choose a primitive d^{th}-root of unity ζ_d, for instance $\zeta_d = e^{2i\pi/d}$.

Definition 1.1. *The Fourier transform $\widehat{f}$ of a function $f : G \to \mathbb{C}$ is the function $\widehat{f} : \widehat{G} \to \mathbb{C}$ given by, for all x in $\widehat{G}$,*

$$\widehat{f}(j) = \tfrac{1}{\sqrt{d}} \sum_{k\in G} f(k)\zeta_d^{jk} \tag{1.1}$$

As we said, the main interesting case in when both j and k belong to $\mathbb{Z}/d\mathbb{Z}$. The matrix F of the Fourier transform in the orthonormal basis $\mathbf{1}_j$ is given by

$$F = \tfrac{1}{\sqrt{p}} (\zeta_d^{jk})_{j,k}. \tag{1.2}$$

The finite Fourier transform on a finite abelian group G has many properties analog to the Fourier transform on $\mathbb{R}$. They are easier to prove. Hence we live them as exercises. We will use the following notation.

The convolution $f*g$ of two functions f and g on G is given by

$$f*g\,(j) \;=\; \sum_{k\in G} f(j-k)\,g(k),$$

for all j in G.

Proposition 1.2. *Let f, g be two functions on the finite abelian group G and $j \in G$.*
a) The Fourier transform is unitary:

$$\sum_{j\in\widehat{G}} \widehat{f}(j)\,\overline{\widehat{g}(j)} = \sum_{k\in G} f(k)\overline{g(k)}. \tag{1.3}$$

b) The inverse Fourier transform is given by

$$\widehat{\widehat{f}}\,(-k) = f(k), \text{for all } k \in G.$$

c) The Fourier transform exchanges convolution and multiplication:

$$\widehat{f*g} \;=\sqrt{p}\,\widehat{f}\,\widehat{g} \;\; \textit{and} \;\; \widehat{f\ g} \;= \tfrac{1}{\sqrt{p}}\,\widehat{f} * \widehat{g}\,.$$

Formula (1.3) is called Plancherel Formula. Replacing g by $\overline{g}$, it can be written as a formula that does not involve complex conjugation:

$$\sum_{j\in\widehat{G}} \widehat{f}(j)\,\widehat{g}(j) = \sum_{k\in G} f(k)g(-k). \tag{1.4}$$

Exercise 1.3. Let G be a finite abelian group and ℓ in $\widehat{G}$.
a) Compute the Fourier transform of the character $\omega_\ell : k \mapsto \zeta_d^{\ell k}$.
b) Let f_ℓ be the translate of the function f by an element $\ell \in G$. This function f_ℓ is given by $f_\ell(j) = f(j-\ell)$ for all j in G.
Prove that $\widehat{f_\ell} \;= \omega_\ell \widehat{f}$ and $\widehat{\omega_\ell f}\,(j) = \widehat{f}\,(j+\ell)$ for all j in G.

Exercise 1.4. Let $a \in (\mathbb{Z}/d\mathbb{Z})^*$ be an invertible element of the ring $G = \mathbb{Z}/d\mathbb{Z}$. Let f be a function on $\mathbb{Z}/d\mathbb{Z}$ and f_a be the function $j \mapsto f(aj)$, for all $j \in \mathbb{Z}/d\mathbb{Z}$. Prove that $\widehat{f_a}\,(j) = \widehat{f}\,(a^{-1}j)$.

1.2 Gauss sums

We know that the Fourier transform has order 4. We want to compute the multiplicity of each of the 4 eigenvalues ± 1 and $\pm i$.

We will need the formula found by Gauss in 1801 that computes the quadratic Gauss sums.

Lemma 1.5. *For $d \geqslant 2$, let $\zeta_d = e^{2i\pi/d}$ and g_d be the normalized quadratic Gauss sum $g_d = \frac{1}{\sqrt{d}} \sum\limits_{1 \leqslant k \leqslant d} \zeta_d^{k^2}$. Then one has*

$$g_d = \frac{1+i^{-d}}{1-i} = \begin{cases} 1 & \text{when } d \equiv 1 \bmod 4, \\ 0 & \text{when } d \equiv 2 \bmod 4, \\ i & \text{when } d \equiv 3 \bmod 4, \\ 1+i & \text{when } d \equiv 0 \bmod 4, \end{cases} \tag{1.5}$$

There are many proof of this formula. The following one is due to Cauchy in 1840.

Proof. For a real nuber t, we denote by $\{t\} := t - [t] \in [0,1)$ its fractional part. We want to comput $g_d = G_d(0)/\sqrt{d}$, where $G_d(t)$ is the function on $\mathbb{R}$ given by

$$G_d(t) = \sum_{0 \leqslant k < d} e^{2i\pi \frac{(k+\{t\})^2}{d}}.$$

This function $G_d(t)$ is 1-periodic, is continuous and is piecewise $\mathcal{C}^1$. Its Fourier coefficients a_n, for $n \in \mathbb{Z}$ are equal to

$$\begin{aligned} a_n &= \int_0^1 G_d(t) e^{-2i\pi n t} \mathrm{d}t = \int_0^d e^{2i\pi \frac{t^2}{d}} e^{-2i\pi n t} \mathrm{d}t \\ &= i^{-n^2 d} \int_{-nd/2}^{-nd/2+d} e^{2i\pi \frac{s^2}{d}} \mathrm{d}s, \end{aligned}$$

where we used the variable $s = t - nd/2$.
The factor $i^{-n^2 d}$ is equal to 1 for n even and to i^{-d} for n odd. Therefore by the inverse theorem for Fourier series, one has

$$G_d(0) = \sum_{n \in \mathbb{Z}} a_n = (1 + i^{-d}) \int_{-\infty}^{\infty} e^{2i\pi \frac{s^2}{d}} \mathrm{d}s.$$

Therefore one gets

$$g_d = G_d(0)/\sqrt{d} = (1 + i^{-d}) \int_{-\infty}^{\infty} e^{2i\pi s^2} \mathrm{d}s.$$

We notice that this semiconvergent integral does not depend on d. We can evaluate it by specializing this equality for $d = 1$, and we obtain $g_d = \frac{1+i^{-d}}{1-i}$ as required. □

It is not so surprising that g_d has this form $a + bi$ with a and b integers, because g_d is the trace of the Fourier transform F that has order 4. Knowing precisely g_d is equivalent to knowing the eigenvalues of F.

Proposition 1.6. *Let $d \geqslant 2$. The eigenvalues with multiplicity of the Fourier transform F on $\mathbb{Z}/d\mathbb{Z}$ are given by the integer* 1 *followed by the sequence $i^{-\ell}$ with $2 \leqslant \ell \leqslant d$.*

This means that the eigenvalues of F are the first d elements of the list: $1, -1, i, 1, -i, -1, i, 1, -i, -1, i, 1, \ldots$

Proof. We only need to check that for $0 \leqslant \ell \leqslant 3$ the trace of the ℓ^{th}-power of the Fourier transform $tr(F^\ell)$ is equal to the sum of the ℓ^{th}-power of this sequence.

One checks that $tr(F^0) = d$ and $tr(F^2) = \begin{cases} 1 & \text{for } d \text{ odd} \\ 2 & \text{for } d \text{ even} \end{cases}$ and one computes $tr(F) = g_d$ and $tr(F^3) = \overline{g_d}$ thanks to Lemma 1.5. □

The following lemma is a variation of Lemma 1.5

Lemma 1.7. *For $d \geqslant 1$, let $\eta_d = -e^{i\pi/d}$. One has the equality*

$$\tfrac{1}{\sqrt{d}} \sum_{1 \leqslant k \leqslant d} \eta_d^{k^2} \quad = \quad e^{-i\pi \frac{d-1}{4}}. \tag{1.6}$$

It is not surprising that the left-hand side c_d has modulus 1 because the Fourier transform is an isometry and the function $g_d : k \mapsto \eta_d^{k^2}$ has Fourier transform $\widehat{g}_d = c_d \, \overline{g_d}$.

Proof. The proof is the same as for Lemma 1.5, with the periodic function

$$G_d(t) = \sum_{0 \leqslant k < d} e^{i\pi \frac{(k+\{t\})^2}{d}} e^{i\pi(k+\{t\})}.$$

whose Fourier coefficients are $a_n = e^{-i\pi d/4} \displaystyle\int_{-nd-d/2}^{-nd+d/2} e^{i\pi \frac{s^2}{d}} \mathrm{d}s$. □

Exercise 1.8. (Fourier transform of the Legendre character) Let p be an odd prime and $\chi_0 : \mathbb{F}_p \to \mathbb{C}$ be the Legendre character

$$\chi_0(k) = \left(\tfrac{k}{p}\right) = \begin{cases} 1 & \text{when } k \neq 0 \text{ is a square,} \\ -1 & \text{when } k \text{ is not a square,} \\ 0 & \text{when } k = 0. \end{cases}$$

a) Prove that $\widehat{\chi_0} = \chi_0$ when $p \equiv 1 \bmod 4$.
b) Prove that $\widehat{\chi_0} = i\chi_0$ when $p \equiv 3 \bmod 4$.
Indication: Use Lemma 1.5.

Exercise 1.9. (Fourier transform of gaussian functions)
Let $G = \mathbb{Z}/d\mathbb{Z}$ with $d \geqslant 2$, $\varepsilon = \pm 1$ and $\eta_d = -e^{i\pi/d}$.
a) Prove that the function $g_\varepsilon : k \mapsto \eta_d^{\varepsilon k^2}$ is well-defined on $\mathbb{Z}/d\mathbb{Z}$.
b) Prove that $\widehat{g_\varepsilon} = e^{-\varepsilon i\pi\frac{d-1}{4}}\, g_{-\varepsilon}$.

Exercise 1.10. Let $G = \mathbb{Z}/d\mathbb{Z}$ with $d \geqslant 2$. For $u \in \{\pm 1, \pm i\}$ a fourth root of unity, we introduce the eigenspace of the Fourier transform $E_u = \{f \in \mathbb{C}[G] \mid \widehat{f} = uf\}$. We denote by $[x]$ the integral part of a real number x.
a) Prove that $\dim E_1 = [\frac{d+4}{4}]$ and $\dim E_{-1} = [\frac{d+2}{4}]$.
b) Prove that $\dim E_i = [\frac{d+1}{4}]$ and $\dim E_{-i} = [\frac{d-1}{4}]$.

The following exercise is a variation on the Genocchi-Schaar equality.

Exercise 1.11. Let c, d be positive integers, $\eta_c = -e^{i\pi/c}$ and $\eta_d = -e^{i\pi/d}$. Prove the following equality that generalizes both (1.5) and (1.6):

$$\frac{1}{\sqrt{d}} \sum_{1 \leqslant k \leqslant d} \eta_d^{ck^2} \;=\; e^{-i\pi\frac{cd-1}{4}} \frac{1}{\sqrt{c}} \sum_{1 \leqslant j \leqslant c} \eta_c^{-dj^2}. \tag{1.7}$$

Indication: The proof is the same as for Lemma 1.5, with the periodic function

$$G_{c,d}(t) = \sum_{0 \leqslant k < d} e^{i\pi\frac{(k+\{t\})^2 c}{d}} e^{i\pi(k+\{t\})c}.$$

1.3 Jacobi symbol

As an application of Gauss formulas, we introduce the Jacobi symbol and prove its reciprocity law. The Jacobi symbol is a natural extension of the Legendre symbol to non-prime integers. The Jacobi symbol is simpler to deal with because when applying the reciprocity law we do not have to factorize the numerator in prime factors.

As before, we set $\zeta_d = e^{2i\pi/d}$. We denote by G the ring $G = \mathbb{Z}/d\mathbb{Z}$ and by $G^* = (\mathbb{Z}/d\mathbb{Z})^*$ its group of units. Its order is the Euler totient $\varphi(d) = d\prod_{p|d}(1-1/p)$.

We recall that the minimal polynomial of ζ_d over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_d(x) := \prod\limits_{c\in G^*}(x-\zeta_d^c)$ whose degree is $\varphi(d)$. The field extension $\mathbb{Q}[\zeta_d]/\mathbb{Q}$ is Galois. Its Galois group is isomorphic to G^*. For $c \in G^*$ we denote by $\sigma_c \in \mathrm{Gal}(\mathbb{Q}[\zeta_d]/\mathbb{Q})$ the corresponding field automorphism defined by the equality $\sigma_c(\zeta_d) = \zeta_d^c$.

In this section, we will only deal with odd integer $d \in \mathbb{Z}$. We introduce the square root of the element $d^* := (-1)^{\frac{d-1}{2}}d$ which is given by the Gauss sum (1.5)

$$\sqrt{d^*} \;=\; i^{\frac{(d-1)^2}{4}}\sqrt{d} \;=\; \begin{cases} +\sqrt{d} & \text{for } d \equiv 1 \bmod 4 \\ +i\sqrt{d} & \text{for } d \equiv 3 \bmod 4 \end{cases} \tag{1.8}$$

According to Gauss formula (1.5), this element belongs to $\mathbb{Q}[\zeta_d]$. Therefore, one has $\sigma_c(\sqrt{d^*}) = \pm\sqrt{d^*}$.

Definition 1.12. *For any odd integer d and any integer c prime to d, the Jacobi symbol $\left(\frac{c}{d}\right) \in \pm 1$ is defined by the equality $\sigma_c(\sqrt{d^*}) = \left(\frac{c}{d}\right)\sqrt{d^*}$*

Remark 1.13. This choice of sign for $\sqrt{d^*}$ is not important for the definition of the Jacobi symbol. It will be useful for the proof of the reciprocity law.

The Jacobi symbols has the following properties.

Proposition 1.14. *Let $d \in \mathbb{Z}$ be an odd integer and $c \in \mathbb{Z}$ be coprime to d.*
a) When $d = \pm 1$, one has $\left(\frac{c}{d}\right) = 1$.
b) When $d = p$ is prime, the Jacobi symbol equals the Legendre symbol:

$$\left(\tfrac{c}{p}\right) = 1 \textit{ if and only if } c \textit{ is a square mod } p.$$

c) When $c = c_1c_2$, one has

$$\left(\tfrac{c}{d}\right) = \left(\tfrac{c_1}{d}\right)\left(\tfrac{c_2}{d}\right).$$

d) When $d = d_1d_2$, one has

$$\left(\tfrac{c}{d}\right) = \left(\tfrac{c}{d_1}\right)\left(\tfrac{c}{d_2}\right).$$

e) When c is also odd, one has the reciprocity law:

$$\left(\tfrac{c}{d}\right)\left(\tfrac{d}{c}\right) = (-1)^{\frac{(c-1)(d-1)}{4}}. \tag{1.9}$$

f) When $c = -1$, one has the first complementary law: $\left(\frac{-1}{d}\right) = (-1)^{\frac{d-1}{2}}$.

g) When $c = 2$, one has the second complementary law: $\left(\frac{2}{d}\right) = (-1)^{\frac{d^2-1}{8}}$.

Proof. *a*) When $d = \pm 1$, One has $\zeta_d = 1$.

b) By Galois theory, since the subextension $\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q}$ has degree 2, the stabilizer $H^* = \{c \in G^* \mid \sigma_c(\sqrt{p^*}) = \sqrt{p^*}\}$ is a subgroup of G^* of index 2. Hence, since G^* is a cyclic group, H^* is the group of squares.

c) This property follows from the equality $\sigma_c = \sigma_{c_1}\sigma_{c_2}$.

d) The field $\mathbb{Q}[\zeta_d]$ contains both $\mathbb{Q}[\zeta_{d_1}]$ and $\mathbb{Q}[\zeta_{d_2}]$, and this property follows from the equality $d^* = d_1^*\, d_2^*$.

e) We write Gauss formula (1.5) for the odd integer cd. The sum is over $j \in \mathbb{Z}/cd\mathbb{Z}$. Since each integer $k \in \mathbb{Z}/cd\mathbb{Z}$ can be written in a unique way as $k = k_1 d + k_2 c$ with $k_1 \in \mathbb{Z}/c\mathbb{Z}$ and $k_2 \in \mathbb{Z}/d\mathbb{Z}$, and since one has the equality $k = k_1^2 d^2 + k_2^2 c^2$ in $\mathbb{Z}/cd\mathbb{Z}$, one gets the following relation between three gauss sums

$$\sum_{1 \leqslant k \leqslant cd} e^{2i\pi k^2/cd} \;=\; \sum_{1 \leqslant k_1 \leqslant c} e^{2i\pi k_1^2 d/c} \sum_{1 \leqslant k_2 \leqslant d} e^{2i\pi k_2^2 c/d}$$

Using Gauss formula (1.5), this can be rewritten as

$$\sqrt{(cd)^*} \;=\; \sigma_c(\sqrt{d^*})\,\sigma_d(\sqrt{c^*}) \;=\; \left(\tfrac{c}{d}\right)\left(\tfrac{d}{c}\right)\sqrt{c^*}\,\sqrt{d^*}.$$

Since $(cd)^* = (-1)^{\frac{(c-1)(d-1)}{4}} c^* d^*$, this gives the reciprocity law (1.9).

e) The Galois transformation σ_{-1} is the complex conjugation. Hence one has $\sigma_{-1}(\sqrt{d^*}) = (-1)^{\frac{d-1}{2}}\sqrt{d^*}$ which is the first complementary law.

g) Since d is odd, Formula (1.6) can be written as

$$\sum_{1 \leqslant k \leqslant d} \eta_d^{k^2} \;=\; i^{-\frac{d-1}{2}}\sqrt{d} \;=\; i^{-\frac{d^2-1}{4}}\sqrt{d^*} \;=\; (-1)^{\frac{d^2-1}{8}}\sqrt{d^*}.$$

Since d is odd, one has $\eta_d = \zeta_d^{(d+1)/2}$ and hence $\sigma_2(\eta_d) = \zeta_d$ and

$$\sigma_2\Big(\sum_{1 \leqslant k \leqslant d} \eta_d^{k^2}\Big) \;=\; \sum_{1 \leqslant k \leqslant c} \zeta_d^{k^2} = \sqrt{d^*}$$

Comparing these two formulas gives $\sigma_2(\sqrt{d^*}) = (-1)^{\frac{d^2-1}{8}}\sqrt{d^*}$, which is the second complementary law. □

We can not avoid to state the quadratic reciprocity in its original form as conjectured by Euler and Legendre and later proved by Gauss.

Corollary 1.15. *Let p and q be odd primes.*
When one of them is equal to 1 *mod* 4*, one has the equivalence*
p is a square mod q if and only if q is a square mod p.
When both of them are equal to 3 *mod* 4*, one has the equivalence*
p is a square mod q if and only if q is not a square mod p.

1.4 Gauss sums and Jacobi sums

In this section we compute the Fourier transform of Dirichlet characters. This will allow us to study Gauss sums and Jacobi sums. As a by product we will give a proof of the two squares theorem.

Let $G = \mathbb{Z}/d\mathbb{Z}$ with $d \geqslant 2$. This group G is also a ring and its set of units $G^* := \{j \in G \mid j \text{ is prime to } d\}$ is an abelian group for the multiplication. The order of G^* is the Euler totient $\varphi(d)$.

Definition 1.16. *A Dirichlet character of G is a map $\chi : G \to \mathbb{C}$ which is a character on G^* and which is zero outside G^*.*

This means that χ is supported by G^*, $\chi(1) = 1$ and $\chi(jk) = \chi(j)\chi(k)$ for all j, k in G^*. We may think of a Dirichlet character as a periodic function on $\mathbb{Z}$.

Definition 1.17. *A Dirichlet character is induced if there exists a Dirichlet character χ' of a proper quotient $G' = \mathbb{Z}/d'\mathbb{Z}$ of $G = \mathbb{Z}/d\mathbb{Z}$ such that $\chi(j) = \chi'(j)$ for all j prime to d.*
A Dirichlet character is primitive if it is not induced.

For instance, when $d = p$ is prime all the Dirichlet characters on G are primitive except the trivial character,

For Dirichlet chacters χ, χ_1, χ_2 , we introduce now the Gauss sum $G(\chi)$ and the Jacobi sum $J(\chi_1, \chi_2)$ by

$$\begin{array}{rcl} G(\chi) & = & \sqrt{d}\,\widehat{\chi}(1) \;=\; \sum_{k \in G} \chi(k)\zeta_d^k, \\ J(\chi_1, \chi_2) & = & \chi_1 * \chi_2(1) \;=\; \sum_{k \in G} \chi_1(1-k)\chi_2(k), \end{array}$$

The primitive Dirichlet characters are those for which the Fourier transform has a simple formula.

Proposition 1.18. *Let χ, χ_1, χ_2 be primitive Dirichlet characters with $\chi_1\chi_2$ also primitive.*
a) The Fourier transform of χ is $\widehat{\chi} = \frac{G(\chi)}{\sqrt{p}}\overline{\chi}$.
b) The Gauss sum has absolute value $|G(\chi)| = \sqrt{d}$.
c) The convolution is given by $\chi_1 * \chi_2 = J(\chi_1,\chi_2)\chi_1\chi_2$.
d) The Jacobi sum is a ratio of Gauss sums $J(\chi_1,\chi_2) = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}$.
e) The Jacobi sum also has absolute value $|J(\chi_1,\chi_2)| = \sqrt{d}$.

Proof. *a*) By exercise 1.4, one has $\widehat{\chi}(ax) = \overline{\chi}(a)\widehat{\chi}(x)$ for all a in G^* and x in G. Hence, since χ is primitive, the Fourier transform $\widehat{\chi}$ is zero outside G^* and therefore is proportional to $\overline{\chi}$. One has $\widehat{\chi} = \widehat{\chi}(1)\,\overline{\chi}$.
b) follows from *a*) and the unitarity of the Fourier transform.
c) and *d*) follow from Fourier applied to the equality $\widehat{\chi_1}\widehat{\chi_2} = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}\widehat{\chi_1\chi_2}$.
e) follows from *b*) and *d*). □

Here is a concrete application of these calculation, which is Fermat's two squares theorem.

Corollary 1.19. *Let p be a prime $p \equiv 1$ mod 4. Then there exists integers a and b such that $p = a^2 + b^2$.*

Proof. Since p is prime, the multiplicative group $\mathbb{F}_p^*$ is cyclic of order $p-1$. Let g_0 be a generator of this group. Since 4 divides $p-1$, there exists a unique Dirichlet character χ on $\mathbb{F}_p$ such that $\chi(g_0) = i = e^{i\pi/2}$. By definition the Jacobi sum $J(\chi,\chi^2)$ belongs to $\mathbb{Z}[i]$. One can write $J(\chi,\chi^2) = a + bi$ with a and b integers. By Proposition 1.18, since the three characters χ, χ^2 and χ^3 are primitive one has $a^2 + b^2 = p$. □

Note that when $p \equiv 3$ mod 4, one cannot write p as a sum of two squares, because 3 is not a sum of two squares in $\mathbb{Z}/4\mathbb{Z}$.

Exercise 1.20. Let χ_1, χ_2, be two Dirichlet characters on $\mathbb{F}_p$.
Prove that $J(\chi_1,\chi_2) = \chi_2(-1)J(\overline{\chi}_1\overline{\chi}_2,\chi_2)$.

1.5 An uncertainty principle

The well known Heisenberg uncertainty principle is a physical principle that says that one cannot know simultaneously with a great precision the position and the speed of a particule. It reflects a classical mathematical inequality: for a function f in the Schwartz space $\mathcal{S}(\mathbb{R})$, one has

$$\|xf\|_{L^2}\ \|f'\|_{L^2}\ \geqslant\ \frac{1}{2}\|f\|_{L^2}^2$$

This inequality [which is a consequence of Cauchy-Schwarz inequality together with an integration by part: $\int|f|^2 = -\int x\overline{f}f' + xf\overline{f}'$] can be restated in terms of the Fourier transform $\widehat{f}$ on the abelian group $\mathbb{R}$. It tells us that

$$\|xf\|_{L^2}\ \|x\widehat{f}\|_{L^2}\ \geqslant\ \frac{1}{2}\|f\|_{L^2}^2$$

This inequality says that f and $\widehat{f}$ cannot both be concentrated near 0.

There is also an uncertainty principle for the Fourier transform on the prime field $\mathbb{F}_p$. For a function f on $\mathbb{F}_p$, we denote its support by

$$\mathrm{supp}(f) = \{x \in \mathbb{F}_p \mid f(x) \neq 0\}.$$

We claim that the support of f and $\widehat{f}$ cannot be simultaneously small.

Proposition 1.21. *Let $f : \mathbb{F}_p \to \mathbb{C}$ be a non-zero function, then one has*

$$\#\,\mathrm{supp}(f) + \#\,\mathrm{supp}(\widehat{f})\ \geqslant\ p{+}1\,. \tag{1.10}$$

This proposition was formulated that way by Biro and Tao in the early 2000's, but was already known to Cebotarev one hundred years ago. The formulation of Cebotarev was more algebraic

Lemma 1.22. (Cebotarev, 1925) *When p is prime, all the minors of the Fourier matrix F are non-zero.*

This means that for all subsets A and B of $\mathbb{F}_p$ with same cardinality, the square submatrices $F_{A,B} = \frac{1}{\sqrt{p}}(\zeta_p^{jk})_{j\in A,k\in B}$ are invertible.

Why Lemma 1.22 implies Proposition 1.21.
This is a simple remark. We denote by A^c the complementary of a subset A in $\mathbb{F}_p$. If a non zero function f has support in a set B and its Fourier transform $\widehat{f}$ has its support in a set A^c with same cardinality $\#A = \#B$, then f gives a non zero element of the kernel of the square submatrix $F_{A,B}$. □

First proof of Lemma 1.22. The following tricky and elementary proof is due to Tao. We denote by $j_1 < \cdots < j_\ell$ the elements of A and by $k_1 < \cdots < k_\ell$ the elements of B. We introduce the polynomial in ℓ variables given by the determinant

$$\Delta(x_1, \ldots, x_\ell) \ := \ \begin{vmatrix} x_1^{k_1} & \cdots & x_1^{k_\ell} \\ \vdots & & \vdots \\ x_\ell^{k_1} & \cdots & x_\ell^{k_\ell} \end{vmatrix}, \tag{1.11}$$

and we introduce the polynomials in 1 variable

$$\Delta_0(x) \ := \ \Delta(x^{j_1}, \ldots, x^{j_\ell}). \tag{1.12}$$

First step We will prove that, setting $L = (\ell-1)\ell/2$, one has

$$\Delta_0(1+y) \ = \ Cy^L + O(y^{L+1}) \ \text{ where } C \in \mathbb{Z} \text{ is coprime to } p. \tag{1.13}$$

Since the polynomial Δ is zero on the hyperplanes $x_m = x_n$, performing successive divisions, we can write

$$\Delta(x_1, \ldots, x_\ell) \ = \ F(x_1, \ldots, x_\ell) \prod_{1 \leqslant m < n \leqslant \ell} (x_n - x_m) \tag{1.14}$$

with $F(x_1, \ldots, x_\ell)$ in $\mathbb{Z}[x_1, \ldots, x_\ell]$. In particular, one has

$$\Delta_0(x) = F_0(x) \prod_{1 \leqslant m < n \leqslant \ell} (x^{j_n} - x^{j_m}),$$

where $F_0(x) \ := \ F(x^{j_1}, \ldots, x^{j_\ell}) \in \mathbb{Z}[x]$. This proves (1.13) except for the congruence condition on the constant C. It remains to prove that

$$F_0(1) \ \neq \ 0 \bmod p. \tag{1.15}$$

For that we plan to give a formula for this quantity $F_0(1) = F(1, \ldots, 1)$. For that, we introduce the differential operator

$$D = (x_1\partial_1)^0 (x_2\partial_2)^1 (x_3\partial_3)^2 \ldots (x_\ell\partial_l)^{\ell-1}. \tag{1.16}$$

We apply this operator to the determinant $\Delta(x_1, \ldots, x_\ell)$, and evaluate the resulting polynomial at the point $(1, \ldots, 1)$.

On the one hand this operator multiplies each coefficient $x_m^{k_n}$ of the matrix in (1.11) by a factor k_n^{m-1}. Therefore one has

$$D\Delta(1,\ldots,1) \;:=\; \begin{vmatrix} k_1^0 & \cdots & k_\ell^0 \\ \vdots & & \vdots \\ k_1^{\ell-1} & \cdots & k_\ell^{\ell-1} \end{vmatrix}. \tag{1.17}$$

One computes easily this Vandermonde determinant

$$D\Delta(1,\ldots,1) \;:=\; \prod_{1\leqslant m<n\leqslant \ell} (k_n - k_m) \;\neq\; 0 \bmod p. \tag{1.18}$$

On the other hand, using the equality (1.14)

$$D\Delta(1,\ldots,1) \;:=\; F(1,\ldots,1) \prod_{1\leqslant m<n\leqslant \ell} (n-m). \tag{1.19}$$

This proves that $F_0(1) \neq 0 \bmod p$ and finishes the first step.

Second step We want to prove that

$$\Delta_0(\zeta_p) \neq 0. \tag{1.20}$$

Assume by contradiction, that $\Delta_0(\zeta_p) = 0$ or equivalently that $F_0(\zeta_p) = 0$. Since the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + \cdots + 1$ is the minimal polynomial of ζ_p over $\mathbb{Q}$, it divides F_0, that is

$$F_0(x) \;=\; \Phi_p(x)\, G_0(x), \tag{1.21}$$

with $G_0(x)$ in $\mathbb{Z}[x]$. In particular, one has

$$F_0(1) \;=\; 0 \bmod p.$$

This contradicts (1.15). □

Exercise 1.23. Prove that a strong uncertainty principle as (1.10) is not valid on an abelian group G whose order d is not prime. Indeed choose f to be the characteristic function $f = \mathbf{1}_H$ of a proper subgroup H of G and check that $\#\operatorname{supp}(f) + \#\operatorname{supp}(\widehat{f}) \leqslant d$.

1.6 Using local fields

Tao's proof is a simplification of Cebotarev's proof. Cebotarev's proof of the first step was based on more explicit calculation. Cebotarev's proof of the second step relied on a few useful and classical facts on local fields that we explain now. By definition a local field is a topological field that is locally compact.

The field $\mathbb{Q}_p$ of p-adic numbers We first recall briefly the definition of the local field $\mathbb{Q}_p$. The field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ for the ultrametric absolute value $|.|_p$ given by $|p^n \frac{a}{b}|_p = p^{-n}$ for all non zero integers a b.

Recall that an absolute value on a field K means a real positive valued map $x \mapsto |x|$ on K such that, $|0| = 0$, $|1| = 1$ and, for all x, y in K

$$|xy| = |x|\,|y| \text{ and } |x+y| \leqslant |x| + |y|. \tag{1.22}$$

It is ultrametric if it satisfies the strenghtened condition $|x+y| \leqslant \max(|x|, |y|)$. By construction, the non zero elements x of $\mathbb{Q}_p$ are the formal sum

$$x = a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \cdots$$

where $n \in \mathbb{Z}$, and all a_m are in $\{0, \ldots, p-1\}$ with $a_n \neq 0$. The ultrametric absolute value $|x| = |x|_{\mathbb{Q}_p}$ of this element x is given by

$$|x|_{\mathbb{Q}_p} = p^{-n}.$$

This defines an ultrametric distance on $\mathbb{Q}_p$ given by $d(x, y) = p^{-\ell}$ where ℓ is the first label where the expansions of x and y differ.

The elements of $\mathbb{N}[\frac{1}{p}]$ are exactly those elements of $\mathbb{Q}_p$ for which the formal sum is finite. This subset $\mathbb{N}[\frac{1}{p}]$ is dense in $\mathbb{Q}_p$. The addition and the multiplication on $\mathbb{N}[\frac{1}{p}]$ extends continuously in a unique way to $\mathbb{Q}_p$. This endows $\mathbb{Q}_p$ with the structure of a topological ring. One checks then that $\mathbb{Q}_p$ is indeed a locally compact field. With this topology, one can reinterpret the formal sums (1.6) as convergent series. The compact subring $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x| \leqslant 1\}$ is called the ring of p-adic integers. It is a principal ring.

p-adic fields By definition a p-adic field is a finite extension of $\mathbb{Q}_p$. We also need a few well known facts on these fields.

For an extension K/K_0 of fields of finite degree $n = [K : K_0]$, the field K is a n-dimensional K_0-vector space. For x in K, the multiplication by x

is an endomorphism m_x of this K_0-vector space. By definition the norm of x is the determinant of this endomorphism.

$$N_{K/K_0}(x) = \det(m_x)$$

Fact 1.24. *Let K be a finite extension of $\mathbb{Q}_p$ of degree n.*
a) There exists a unique absolute value $|.| = |.|_K$ on K satisfying (1.22) *that extends the absolute value of $\mathbb{Q}_p$. It is given by*

$$|x|_K = |N_{K/\mathbb{Q}_p}(x)|_{\mathbb{Q}_p}^{1/n}.$$

b) The topological field K is then a locally compact field.
c) The set $\mathcal{O}_K = \{x \in K \mid |x| \leqslant 1\}$ is a principal ring which is both compact and open. It is called the ring of integers.
d) The set $\mathfrak{m}_K = \{x \in K \mid |x| < 1\}$ is a principal ideal of $\mathcal{O}_K$ which is both open and compact.

Fact 1.25. *a) When π is a uniformizer, i.e. when $\mathfrak{m}_K = \pi\mathcal{O}_K$, one has $|\pi| = p^{-1/e}$ for an integer $e \geqslant 1$ called the ramification index of $K/\mathbb{Q}_p$.*
b) Let κ be the residual field of K, that is the quotient $\kappa := \mathcal{O}_K/\mathfrak{m}_K$. It is a finite extension of the residual field $\mathbb{F}_p := \mathbb{Z}_p/p\mathbb{Z}_p$ of $\mathbb{Q}_p$. The degree f of the extension $\kappa/\mathbb{F}_p$ is called the inertia index.
c) One has the equality $n = ef$.

The finite extension $[K/\mathbb{Q}_p]$ is said to be totally ramified if $f = 1$ and totally unramified if $e = 1$.

The following fact tells us that one can deal with elements of a number field in a very concrete way, very much like with the p-adic numbers.

Fact 1.26. *Let K be a finite extension of $\mathbb{Q}_p$, let e be its ramification index, let $q = p^f$ be the cardinality of its residual field κ, let π be a uniformizer of K and let $S \subset \mathcal{O}_K$ be a subset of cardinality q containing 0 such that $\mathcal{O}_K = S + \pi\mathcal{O}_K$.*
a) The non zero elements x of K can be written in a unique way as

$$x = s_n\pi^n + s_{n+1}\pi^{n+1} + s_{n+2}\pi^{n+2} + \cdots$$

where $n \in \mathbb{Z}$, and all s_m are in S with $s_n \neq 0$.
b) The absolute value $|x| = |x|_K$ of this element x is given by

$$|x|_K = p^{-n/e}.$$

A ramified cyclotomic extension of $\mathbb{Q}_p$ We are now ready to understand Cebotarev's proof. It will rely on the following lemma. Instead of considering the primitive p^{th}-root of unity ζ as an element of $\mathbb{C}$ we now consider it as an element of the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$

Lemma 1.27. *Let $K = \mathbb{Q}_p[\zeta]$ be the extension of $\mathbb{Q}_p$ obtained by adding a primitive p^{th}-root of unity ζ.*
a) Then K is an extension of $\mathbb{Q}_p$ of degree $p-1$.
b) This extension is totally ramified: its residual field is $\mathbb{F}_p$.
c) The element $\pi := \zeta - 1$ is a uniformizer: one has $|\pi| = p^{-1/(p-1)}$.

Proof of Lemma 1.27. We will give two proofs of Point *a*).

a) Let

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1$$

be the cyclotomic polynomial. We want to prove that this polynomial is irreducible over $\mathbb{Q}_p$. The polynomial

$$F(y) = \Phi_p(y+1) = y^{p-1} + \tbinom{p}{p-1} y^{p-2} + \cdots + \tbinom{p-1}{2} y + p$$

is an Eisenstein polynomial. This means that all its coefficients are prime to p except the last one which is divisible by p but not by p^2. By the Eisenstein criterion, such a polynomial is always irreducible over $\mathbb{Q}_p$.

a), *b*) and *c*) The element $\pi = \zeta - 1$ is a root of F. The elements $\pi_i = \zeta^i - 1$ are also roots of F, for $0 < i < p$. Since the ratios π_i/π and π/π_i are in $\mathcal{O}_K$, all the absolute values $|\pi_i|$ are equal. Since the product of these roots is

$$\pi_1 \cdots \pi_{p-1} = (-1)^{p-1} p,$$

one gets $|\pi| = p^{\frac{-1}{p-1}}$. This proves that the ramification index of $K/\mathbb{Q}_p$ is $p-1$, and that π is a uniformizer. This also proves that the degree $[K : \mathbb{Q}_p]$ is $p-1$. □

Cebotarev's proof of Proposition 1.21.
The first step of the proof is the same. We introduce the polynomial $\Delta_0(x)$ in one variable given by the determinant

$$\Delta_0(x) := \begin{vmatrix} x^{j_1 k_1} & \cdots & x^{j_1 k_\ell} \\ \vdots & & \vdots \\ x^{j_\ell k_1} & \cdots & x^{j_\ell k_\ell} \end{vmatrix}$$

We want to prove that $\Delta_0(\zeta_p) \neq 0$. Let $L = (\ell - 1)\ell/2$. We know by the calculation (1.13) in the first step of the proof that

$$\Delta_0(1 + y) \;=\; Cy^L + O(y^{L+1}) \text{ where } C \in \mathbb{Z} \text{ is coprime to } p.$$

The key idea for the second step in this proof is to reinterpret this equality in the local field $K = \mathbb{Q}_p[\zeta]$ where ζ is a primitive p^{th} root of unity. According to Lemma 1.27, one has $\zeta = 1 + \pi$ where the element π is a uniformizer in K. Hence one has

$$\Delta_0(\zeta) \;\in\; C\pi^L + \pi^{L+1}\mathcal{O}_K,$$

where $\mathcal{O}_K$ is the ring of integers of K. Since the integer C is prime to p, this implies that $|\Delta_0(\zeta)| = |\pi^L| = p^{-L/(p-1)}$. In particular, one has $\Delta_0(\zeta) \neq 0$. □

Exercise 1.28. *a*) Compute the expansion of $x = -1$ in $\mathbb{Q}_3$.
b) Compute the expansion of $x = 1/2$ and $x = -1/2$ in $\mathbb{Q}_7$.
c) Compute the expansion of $x = 1/3$ and $x = -1/3$ in $\mathbb{Q}_{11}$.
d) Prove that an element x in $\mathbb{Q}_p$ has an ultimately periodic expansion if and only if x is rational.

Exercise 1.29. Let p be an odd prime.
a) Show that the group of squares $(\mathbb{Q}_p^*)^2$ is a subgroup of index 4 in the multiplicative group $\mathbb{Q}_p^*$.
b) Prove that $\mathbb{Q}_p$ has exactly 3 quadratic extensions.
c) How many are ramified?

Exercise 1.30. Let K be a p-adic field and $\mathcal{O}_K$ its ring of integers. Prove that an element $x \in \mathcal{O}_K$ is invertible in $\mathcal{O}_K$ if and only if $|x| = 1$. Such an x is called a unit. The group of units is denoted $\mathcal{O}_K^*$.

Exercise 1.31. Let $\ell \geqslant 2$ and $K = \mathbb{Q}_p[y]$ where $y^\ell = p$.
a) Show that K is an extension of $\mathbb{Q}_p$ of degree ℓ.
b) Show that this extension is totally ramified.

Exercise 1.32. (Hensel lemma) Let K be a p-adic field, $\mathcal{O}_K$ its ring of integers, and κ its residual field. Let $F[X] \in \mathcal{O}_K[X]$ be a unitary polynomial of degree d and $\overline{F}(X) \in \kappa[X]$ be its reduction modulo $\mathfrak{m}_K$. Assume that $\overline{F}(X)$ has d distinct roots in κ. Show that, for every root $\xi \in \kappa$ of $\overline{F}$, there is a unique root x of F in $\mathcal{O}_K$ that lifts ξ.
Indication: apply Newton method to obtain better and better approximate roots of F starting from any lift of ξ.

Exercise 1.33. (Unramified extensions) Let K be a finite extension of $\mathbb{Q}_p$, e its inertia degree, κ its residual field and $q = p^e$.
a) Show that the equation $x^q = x$ has q roots in K.
Indication: use Hensel Lemma.
b) Let $K_0 \subset K$ be the subfield spanned by the $(q-1)^{\text{th}}$-roots of unity. Prove that K_0 is a Galois extension of $\mathbb{Q}_p$ of degree e.
c) Prove that the extension $K_0/\mathbb{Q}_p$ is totally unramified while the extension K/K_0 is totally ramified.

Notes to Chapter 1. [44] and [43].

2 Biunimodular functions

The aim of this lecture is to introduce a family of functions on $\mathbb{Z}/d\mathbb{Z}$ called biunimodular that have properties very similar to the gaussian functions. They are part of a larger family called $\mathcal{H}$-functions.

We first give equivalent definitions and a few examples.

We then prove that, when $d = p$ is prime, there are only finitely many $\mathcal{H}$-functions. We give a formula for this number of $\mathcal{H}$-functions.

2.1 Definition and properties

Let G be a finite abelian group.

Definition 2.1. *A function $f : G \to \mathbb{C}$ is unimodular if $|f(\ell)| = 1$ for all $\ell \in G$. The function f is biunimodular if both f and its Fourier transform $\widehat{f}$ are unimodular.*

It is natural to extend Definition 2.1

Definition 2.2. *A function $f : G \to \mathbb{C}$ is a $\mathcal{H}$-function if there exists $g : G \to \mathbb{C}$ such that*

$$f\,\check{g} = 1 \text{ and } \widehat{f}\,\widehat{g} = 1. \tag{2.1}$$

Here the function $\check{g}$ is the function $\check{g}(k) = g(-k)$.

When f is unimodular, one has the equivalence

f is biunimodular if and only if f is a $\mathcal{H}$-function.

Indeed when $g(k) = \overline{f(-k)}$, one has $\widehat{g}(k) = \overline{\widehat{f}(k)}$.

The biunimodular functions, with $G = C_d$ are interesting in transmission theory, because of the following property

Lemma 2.3. *A unimodular function $f : G \to \mathbb{C}$ is biunimodular if and only if one has*

$$\sum_{k \in G} f(k+\ell)\,\overline{f(k)} \;=\; 0 \quad \textit{for all } \ell \in G,\ \ell \neq 0. \tag{2.2}$$

Geometrically, Condition (2.2) means that the translates of f form an orthogonal basis of $\ell^2(G)$.

Lemma 2.3 is a consequence of the following lemma that gives an equivalent definition for $\mathcal{H}$-functions.

Lemma 2.4. *A function $f\!:\!G\!\to\!\mathbb{C}^*$ is a $\mathcal{H}$-function if and only if*

$$\sum_{k\in G} f(k\!+\!\ell)/f(k) \;=\; 0 \quad \textit{for all } \ell \in G,\ \ell \neq 0.. \tag{2.3}$$

Proof of Lemma 2.4. Let $f : G \to \mathbb{C}^*$ be a non-vanishing function on G and set $g := 1/\check{f}$. Since the function $\sqrt{d}\,\widehat{f}\,\widehat{g}$ is the Fourier transform of the convolution $f * g$, Equation (2.1) is equivalent to

$$f\,\check{g} = 1 \;\text{ and }\; f * g = d\,\delta_0 .$$

Taking into account the Plancherel formula (1.4), this last condition is equivalent to Condition (2.3). □

A $\mathcal{H}$-function is said to be normalized if $f(0) = 1$. By multiplying a $\mathcal{H}$-function by a scalar one can always normalize it.

Exercise 2.5. A cyclic d-root is a function $z : C_d \to \mathbb{C}$ such that,

$$\sum_{j\in C_d} z_j \cdots z_{j+\ell} = 0 \text{ for } 0 < \ell < d \text{ and } \quad z_1 \cdots z_d = 1.$$

Check that the formula $z_j = f(j\!+\!1)/f(j)$ induces a bijection between the set of $\mathcal{H}$-functions f with $f(0) = 1$ and the set of cyclic d-roots z.

Finding explicitely all the cyclic d-roots was a challenge test for computer formal calculation and algorithms around 2000, where the case $d = 9$ and $d = 10$ was found by Faugère in [19].

2.2 Elementary biunimodular functions

The notion of biunimodular functions was introduced by Per Enflo in the 80's in relation with the "circulant complex Hadamard matrices".

Gaussian functions The simplest examples of biunimodular functions on $G = \mathbb{Z}/d\mathbb{Z}$ with $d \geqslant 2$ are the gaussian functions as in Exercise 1.9. Let $\eta_d = -e^{i\pi/d}$. Those are the functions of the form

$$g_{a,\ell} : k \mapsto \eta_d^{ak^2+2\ell k} \tag{2.4}$$

for some a in $(\mathbb{Z}/d\mathbb{Z})^*$ and ℓ in $\mathbb{Z}/d\mathbb{Z}$.

When $d = p$ is prime there are $(p-1)p$ gaussian functions.

Björckian functions Per Enflo asked for the existence of other biunimodular functions, when $d = p > 2$ is prime. Björck answered in 1989 by classifying in [16] the biunimodular functions h that are invariant by multiplication by squares.

Indeed writing $h = \delta_0 + a\,\mathbf{1}_{\mathbb{F}_p^*} + b\chi_0$, with χ_0 the Legendre character. one computes $\widehat{h} = \frac{1-a+pa}{\sqrt{p}}\delta_0 + \frac{1-a}{\sqrt{p}}\,\mathbf{1}_{\mathbb{F}_p^*} + b\widehat{\chi_0}$ Using exercise 1.8, one compute $\widehat{\chi_0}$.

When $p \equiv 1 \bmod 4$, one has $\widehat{\chi_0} = \chi_0$ and there are four such biunimodular functions: the following two functions $h_\pm$ and their complex conjugates.

$$h_\pm = \delta_0 + \tfrac{1}{1\pm\sqrt{p}}\,\mathbf{1}_{\mathbb{F}_p^*} + i\tfrac{\sqrt{p\pm 2\sqrt{p}}}{1\pm\sqrt{p}}\,\chi_0,$$

These functions are even and satisfy $\widehat{h_\pm} = h_\pm$.

When $p \equiv 3 \bmod 4$ one has $\widehat{\chi_0} = i\chi_0$ there are four such biunimodular functions: the following two even functions $h_\pm$ and their complex conjugates

$$h_\pm = \delta_0 + \tfrac{1}{1+i\sqrt{p}}\,\mathbf{1}_{\mathbb{F}_p^*} \pm i\,\tfrac{\sqrt{p}}{1+i\sqrt{p}}\,\chi_0.$$

We introduce the slight variations $h_{\pm,j,k}$ of these functions, where $j, k \in \mathbb{F}_p$,

$$h_{\pm,j,k} : \ell \mapsto e^{2i\pi j\ell/p}\,h_\varepsilon(\ell + k). \tag{2.5}$$

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

Exercise 2.6. Let $u \in \mathbb{C}$ with $|u| = 1$ and let $j = e^{\frac{2i\pi}{3}}$.
a) Prove that the function $(1, u, -1, u)$ is biunimodular on C_4.
b) Prove that $(1, 1, u, j, j^2, u, j^2, j, u)$ is biunimodular on C_9.
c) Prove that there exist infinitely many normalized biunimodular functions on C_d when $d = p^r$ is a prime power with $r \geqslant 2$.
d) Extend this assertion to the case where d has a square divisor.

Exercise 2.7. Let f_1 and f_2 be two biunimodular functions respectively on two finite abelian groups G_1 and G_2. Prove that the product function f given by $f(k_1, k_2) = f_1(k_1)f_2(k_2)$ is a biunimodular function on $G_1 \times G_2$.

2.3 Finiteness of biunimodular functions

The aim of this section is to prove the following theorem due to Haagerup in 2008 .

Theorem 2.8. *When p is prime, the set of normalized $\mathcal{H}$-functions is finite.*

From this theorem, one deduce directly the following corollary. Note that it is not clear how one could prove the corollary without proving first the whole Theorem 2.8.

Corollary 2.9. *When p is prime, the set of normalized biunimodular functions is finite.*

The proof of Theorem 2.8 relies on the following proposition.

We introduce the vectorspace $E = \mathbb{C}[\mathbb{F}_p]$ and its affine subspace

$$E_1 := \{f \in \mathbb{C}[\mathbb{F}_p] \mid f(0) = 1\}.$$

We also introduce the affine space

$$F_1 := \{(f_0, g_0) \in E \times E \mid f_0(0) = 1 \text{ and } \sum_{x\in\mathbb{F}_p} f_0(x) = \sum_{x\in\mathbb{F}_p} g_0(x)\ \}.$$

Note that $\dim(F_1) = 2\dim(E_1) = 2p - 2$.

Proof. The map

$$\begin{array}{rcl} \Phi : E_1 \times E_1 & \longrightarrow & F_1 \\ (f, g) & \mapsto & (f\,\check{g}, \widehat{f}\,\widehat{g}) \end{array} \tag{2.6}$$

is a well-defined proper map. □

This means that the inverse image $\Phi^{-1}(K)$ of a compact set K of $E \times E$ is a compact set. The presence of $\check{g}$ in the formula is not important for the properness of Φ. But this is what we need for the proof of Theorem 2.8. The fact that the image is included in F_1 will play a crucial role in Theorem 2.17.

Proof of Proposition 2.3. Using the Plancherel formula (1.4), we first note that by $\Phi(E_1 \times E_1)$ is included in F_1.

Let f_n and g_n be sequences in $E_{\geqslant 1}$ such that

$$\Phi(f_n, g_n) \text{ is bounded.} \tag{2.7}$$

We want to prove that both f_n and g_n are bounded. Assume by contradiction that one of them is not bounded. This implies that

$$\lim_{n\to\infty} \|f_n\|\,\|g_n\| = \infty, \tag{2.8}$$

where $\|f\|$ is any norm on E. We introduce the functions

$$u_n = \frac{f_n}{\|f_n\|} \text{ and } v_n = \frac{g_n}{\|g_n\|}.$$

After extraction, one can assume that these sequences of functions converge to two non zero functions

$$u_\infty = \lim_{n\to\infty} u_n \text{ and } v_\infty = \lim_{n\to\infty} v_n.$$

Since the Fourier transform is continuous one gets

$$\widehat{u}_\infty = \lim_{n\to\infty} \widehat{u}_n \text{ and } \widehat{v}_\infty = \lim_{n\to\infty} \widehat{v}_n.$$

Therefore Equality (2.8) implies that

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

This implies that both

$$\begin{aligned} \#\,\mathrm{supp}(u_\infty) + \#\,\mathrm{supp}(v_\infty) &\leqslant p \qquad \text{and} \\ \#\,\mathrm{supp}(\widehat{u}_\infty) + \#\,\mathrm{supp}(\widehat{v}_\infty) &\leqslant p\,. \end{aligned}$$

These inequalities contradict the uncertainty principle (1.10) either for u_∞ or for v_∞. □

2.4 Using dominant morphisms

To go on our understanding of biunimodular functions, we will need a useful and classical theorem from complex algebraic geometry.

We recall a few basic definitions. A Zariski closed subset $X \subset \mathbb{C}^d$ is the set of zeros of a family of polynomials on $\mathbb{C}^d$. Such a subset is also called an *affine algebraic variety* or an *algebraic subvariety of* $\mathbb{C}^d$. One denotes by $\mathbb{C}[X]$ the algebra of algebraic functions on X. Those are the restrictions to X of polynomial functions on $\mathbb{C}^d$.

A Zariski open set $U \subset \mathbb{C}^d$ is the complementary of a Zariski closed set. This defines a topology on $\mathbb{C}^d$ called the Zariski topology.

For instance, a non empty Zariski open subset of $\mathbb{C}$ has finite complementary.

An algebraic morphism $\varphi : X \to Y$ between two affine algebraic varieties is a map whose coordinate maps are given by algebraic functions on X. Such a morphism induces an algebra morphism $\varphi^* : \mathbb{C}[Y] \to \mathbb{C}[X]$ given by $\varphi^*(F) = F \circ \varphi$.

Definition 2.10. *An algebraic morphism $\varphi : X \to Y$ between two affine algebraic varieties is called dominant if its image $\varphi(X)$ is Zariski dense in Y or, equivalently, if the map φ^* is injective.*

The following fact due to Chevalley is the main result of abstract elimination theory.

Fact 2.11. *Let $\varphi : X \to Y$ be a dominant morphism between two algebraic varieties. Then the image $\varphi(X)$ contains a non empty Zariski open subset U of Y.*

More precisely the image $\varphi(X)$ is *constructible*. This means that $\varphi(X)$ is a finite union of Zariski locally closed sets Z_m. We recall that a Zariski locally closed set is by definition the intersection of a Zariski closed and a Zariski open set.

A strong improvement of Fact 2.11 is to work with projective algebraic varieties X and Y. The conclusion in this case is that the image is closed.

Remark 2.12. From the point of view of logic, Fact 2.11 is called the elimination of quantifier in an algebraically closed field, and in this context it is due to Tarski.

Remark 2.13. A concrete point of view on elimination theory is given by the notion of resultant polynomial. Another concete point of view on elimination theory that gives rise to efficient algorithms, is given by the notion of Gröbner basis.

Sketch of proof of Fact 2.11. One does not think of X as an algebraic subvariety of $\mathbb{C}^d$ but as an algebraic subvariety of $Y \times \mathbb{C}^d$ so that the map φ is nothing but the projection on the first component.

This is very useful because, by an induction argument, one can now reduce to the case where $d = 1$. In this case, one can write

$$X = \{(y,t) \in Y \times \mathbb{C} \mid P_0(y,t) = P_1(y,t) = \ldots = P_\ell(y,t) = 0\}. \tag{2.9}$$

where the P_i are polynomials.

We know that two polynomials in t have a common root if and only if their resultant is non zero. The rough strategy is then to say that, for all i, the resultant $R_i(y)$ of $P_0(y,t)$ and $P_i(y,t)$ is zero on a Zariski dense subset of Y, hence on the whole of Y and hence, for all y, the polynomial $P_0(y,t)$ and $P_i(y,t)$ have a common root $t_{y,i}$, which gives an element $(y, t_{y,i})$ of X above y. There are two drawbacks in this rough strategy.
(i) The first one is that this root $t_{y,i}$ of P_0 may depend on i.
(ii) The second one is that the resultant of two polynomials depends polynomially on their coefficients only among the polynomials of fixed degree.

It is easy to circumvent these two issues.
For (i), we introduce the polynomials $P_\alpha(y,t) := \sum\limits_{1\leqslant i\leqslant \ell} \alpha_i P_i(y,t)$ with $\alpha \in \mathbb{C}^\ell$.
For (ii) we write $P_0 = \sum\limits_{0\leqslant k\leqslant \delta_0} a_k(y)t^k$ and $P_\alpha = \sum\limits_{0\leqslant k\leqslant \delta} b_k(\alpha,y)t^k$ where δ_0 is the degree in t of P_0 and δ is the maximum degree in t of the P_α. We introduce the Zariski open set $U := \{y \in Y \mid a_{\delta_0}(y) \neq 0 \text{ and } b_\delta(\alpha,y) \not\equiv 0\}$, so that, for all y in U, the Zariski open set $V_y := \{\alpha \in \mathbb{C}^\ell \mid a_{\delta_0}(y) \neq 0 \text{ and } b_\delta(\alpha,y) \neq 0\}$ is non empty. For y in U and α in V_y the resultant $R_\alpha(y)$ of $P_0(y,t)$ and $P_\alpha(y,t)$ is a polynomial in both α and y.

By asumption for y in a Zariski dense subset of U, these polynomials $R_\alpha(y)$ are zero. Hence these polynomials are identically 0. Since $t \mapsto P_0(y,t)$ have only finitely many roots, this implies that, for all y in U, I can find a root t_y of $P_0(y,t)$ which is is also a root of $P_\alpha(y,t)$ for a Zariski dense set of values of α. This point (y,t_y) is then an element of X above y. □

Corollary 2.14. *Let $X \subset \mathbb{C}^d$ be an algebraic subvariety. If X is bounded, then X is finite.*

Proof of Corollary 2.14. Assume that X is infinite. Then there exists a coordinate map $p_\ell : X \to \mathbb{C}$ with $1 \leqslant \ell \leqslant d$, whose image $p_\ell(X)$ is unbounded. Therefore this map p_ℓ is dominant. By Fact 2.11, this image contains a Zariski open subset of $\mathbb{C}$. This means that $p_\ell(X)$ is the complementary of a finite set. In particular X is not bounded. □

Proof of Theorem 2.8. Let $E_1 := \{f \in \mathbb{C}[\mathbb{F}_p] \mid f(0) = 1\}$. According to Proposition 2.3 the algebraic variety

$$\mathcal{R} := \{(f,g) \in E_1 \times E_1 \mid f\,\check{g} = 1 \text{ and } \widehat{f}\widehat{g} = 1\} \tag{2.10}$$

is compact. Therefore by Corollary 2.14 this variety is finite. Hence the set of $\mathcal{H}$-functions is also finite. □

Exercise 2.15. Let p be prime and N be a non negative function on $\mathbb{F}_p$ with $N(0) = 1$.
a) Prove that the set $\mathcal{E}_N$ of complex valued functions f on $\mathbb{F}_p$ with $f(0) = 1$ and $|f(x)| = |\widehat{f}(x)| = N(x)$, for all x in $\mathbb{F}_p$, is a finite set.
b) Prove that there exists $\varepsilon > 0$ such that if $N < \varepsilon$ on $\mathbb{F}_p^*$, this set $\mathcal{E}_N$ is empty.
c) Prove that $\varepsilon \leqslant \frac{1}{\sqrt{p}+1}$.
d) Prove that one can choose $\varepsilon = \frac{1}{2(\sqrt{p}+1)}$.

2.5 Using proper morphisms

To go on our understanding of biunimodular functions, we will need another useful and classical theorem from complex analytic geometry. 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 [45, p.148].

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

Fact 2.16. *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 :* $\quad N(\Psi_t, B) := \sum\limits_{\{z\in\overline{B} | \Psi_t(z)=0\}} m_z(\Psi_t)$ *does not depend on* t.

Sketch of proof of Fact 2.16. See [21, Section 5.2] or [1, Thm 2.5]. There are integral formulas for the number $N(\Psi, B) := \sum\limits_{\{z\in\overline{B} | \Psi(z)=0\}} m_z(\Psi)$ of zeros counted with multiplicity in the ball $\overline{B}$ for a holomorphic map $\Psi : \Omega \to \mathbb{C}^d$ that does not vanish on ∂B. These formulas tell us that the integer $N(\Psi_t, B)$ depends continuously on t and hence is constant.

When $m = 1$ this is the famous "argument principle" due to Cauchy in 1830 which says that

$$N(\Psi, B) \; = \; \frac{1}{2i\pi} \int_{\partial B} \frac{\Psi'(z)}{\Psi(z)} \, \mathrm{d}z \, .$$

When $m \geqslant 1$, the Cauchy formula has been extended by Bochner-Martinelli. The formula expresses this number as the integral of a $2m-1$ differential form on a $(2m-1)$-dimensional sphere:

$$N(\Psi, B) \; = \; \frac{(m-1)!}{(2i\pi)^m} \frac{1}{|\Psi|^2} \int_{\partial B} \sum_{1\leqslant j\leqslant m} (-1)^{j-1} \overline{\Psi}_j \mathrm{d}\overline{\Psi}_{[j]} \mathrm{d}\Psi \, ,$$

where $|\Psi|^2 = \sum\limits_{1\leqslant j\leqslant m} |\Psi_j|^2$, where $\mathrm{d}\overline{\Psi}_{[j]} := \mathrm{d}\overline{\Psi}_1 \cdots \widehat{\mathrm{d}\overline{\Psi}_j} \cdots \mathrm{d}\overline{\Psi}_\ell$ with $\mathrm{d}\overline{\Psi}_j$ omitted and where $\mathrm{d}\Psi := \mathrm{d}\Psi_1 \cdots \mathrm{d}\Psi_\ell$. □

2.6 Counting biunimodular functions

Haagerup proved more than merely the finiteness of biunimodular functions on $\mathbb{F}_p$. He gave a formula for number of $\mathcal{H}$-functions.

Theorem 2.17. (Haagerup) *Let p be prime. Then, counted with multiplicities, the number of normalized $\mathcal{H}$-functions on $\mathbb{F}_p$, is equal to the binomial coefficient $\binom{2p-2}{p-1}$.*

Remark 2.18. It seems but it is not proved that, in this case, the multiplicities are equal to 1.

The key point will be a deformation argument using the map Φ as in Proposition 2.3. Since this holomorphic map is proper between affine spaces of same dimension, the number of points in its fibers, counted with multiplicities is constant. This follows from Fact 2.16 applied to the maps

$$\begin{array}{rcl} \Psi_t : E_1 \times E_1 & \longrightarrow & F_0 \\ (f,g) & \mapsto & \Phi(f,g) - (\delta_0 + t\mathbf{1}_{\mathbb{F}_p^*}, \delta_0 + t\mathbf{1}_{\mathbb{F}_p^*}) \end{array} \tag{2.11}$$

where

$$F_0 := \{(f_0, g_0) \in E \times E \mid f_0(0) = 0 \text{ and } \sum_{x \in \mathbb{F}_p} f_0(x) = \sum_{x \in \mathbb{F}_p} g_0(x) \}.$$

Hence we can perform the counting for a simpler fiber. In the following lemma we study in great detail the fiber of Φ over the point (δ_0, δ_0).

Lemma 2.19. *Let Φ be the map* (2.6).
a) For every subsets A, B of $\mathbb{F}_p$ containing 0 *such that*

$$\#A + \#B = p + 1, \tag{2.12}$$

there exists a unique function $f_{A,B} \in E_1$ with support A whose Fourier transform $\widehat{f}_{A,B} \in E$ has support B.
b) We set $g_{A,B} \in E_1$ to be the function $g_{A,B} := f_{-A',B'}$ where A' and B' are defined by $A \cup A' = B \cup B' = \mathbb{F}_p$ and $A \cap A' = B \cap B' = \{0\}$. Then one has

$$\Phi(f_{A,B}, g_{A,B}) = (\delta_0, \delta_0).$$

c) Every point in the fiber $\Phi^{-1}(\delta_0, \delta_0)$ is one of these points $(f_{A,B}, g_{A,B})$.
d) The number of points in this fiber $\Phi^{-1}(\delta_0, \delta_0)$ is equal to $\binom{2p-2}{p-1}$.
e) The map Φ is non-degenerate at each of the points $(f_{A,B}, g_{A,B})$ of the fiber $\Phi^{-1}(\delta_0, \delta_0)$.

Proof of Lemma 2.19. a) For a subset A of $\mathbb{F}_p$ of cardinality n_A, we denote by $\mathbb{C}[A]$ the space of functions on A. It has dimension n_A.

As a consequence of Inequality (1.10), for any subsets A_0 and B_0 of $\mathbb{F}_p$ with $n_{A_0} + n_{B_0} = p$, the map

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

is an isomorphism.

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

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

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 $f_{A,B}(0) = 1$. 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 one has $f\check{g} = \delta_0$.

Similarly, one has $\widehat{f}\,\widehat{g} = \lambda\delta_0$ for some constant λ. This constant λ is equal to 1 by the Plancherel formula.

c) Conversely, let $(f,g) \in E_1 \times E_1$ such that $f\check{g} = \delta_0$ and $\widehat{f}\widehat{g} = \delta_0$. Set $A := \mathrm{supp}(f)$, $B := \mathrm{supp}(\widehat{f})$, $A' := \mathrm{supp}(\check{g})$ and $B' := \mathrm{supp}(\widehat{g})$. By assumption, one has $A \cap A' = B \cap B' = \{0\}$. In particular, one has

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

By inequality (1.10), one has

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

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

d) By Point *c*), the fiber $\Phi^{-1}(\delta_0, \delta_0)$ is in bijection with the set of pairs $(A \smallsetminus \{0\}, B \smallsetminus \{0\})$ of subsets of $\mathbb{F}_p \smallsetminus \{0\}$ such that $n_{A\smallsetminus\{0\}} + n_{B\smallsetminus\{0\}} = p - 1$. Their total number is $\binom{2p-2}{p-1}$ as announced.

e) Fix a point $(f,g) = (f_{A,B}, \overline{f}_{A',-B'})$ in the fiber $\Phi^{-1}(\delta_0, \delta_0)$. 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 functions such that $\varphi(0) = \psi(0) = 0$. Assume that (φ, ψ) is in the kernel of $D\Phi(f,g)$. The formula for the differential is

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

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

$$\mathrm{supp}(\varphi) \subset A \smallsetminus \{0\} \ \text{ and } \ \mathrm{supp}(\psi) \subset -A' \smallsetminus \{0\}.$$

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

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

In particular one gets

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

Therefore, by the uncertainty inequality in Proposition 1.21, one has $\varphi = \psi = 0$.

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

Proof of Theorem 2.17. Since the family of holomorphic maps Ψ_t in (2.11) is proper, by Fact 2.16, the number of points in $\Psi_t^{-1}(w)$, counted with multiplicities is constant. We want to prove that, counted with multiplicity, the number of points in the fiber $\Phi^{-1}(1, 1)$ is equal to $\binom{2p-2}{p-1}$. It is then equivalent to prove it for the fiber $\Phi^{-1}(\delta_0, \delta_0)$. This was done in the previous Lemma 2.19. □

Remark 2.20. It would be nice to have a similar counting formula for all biunimodular functions f on $\mathbb{F}_p$ with $f(0) = 1$.

Notes to Chapter 2.

The example in Section 2.2 is due to Björck [16] The finiteness and the counting results are due to Haagerup in [22, Sec. 4].

3 Clifford tori

The aim of this lecture is to explain why there exist biunimodular functions that are neither Gaussian functions nor Björckian functions. We will also explain a similar construction with the odd-biunimodular functions.

What is appealing in these results is that, in spite of the simplicity of their statement and on the algorithmic complexity of the construction, the proof mixes arguments from Symplectic geometry (Intersection of Clifford tori), Number theory (Stickelberger formula for Jacobi sums) and Complex analysis (Multiplicity of holomorphic maps) that have their origin in very different problems.

3.1 Using Clifford tori

We first need to explain a fact whose statement looks elementary but whose proof relies on symplectic geometry.

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

Fact 3.1. *Let $\mathbb{CP}^{n-1}$ be the complex projective space, let $\mathbb{T}^{n-1} \subset \mathbb{CP}^{n-1}$ be the Clifford torus, and let $u \in U$ be a unitary transformation.*
a) The intersection $\mathbb{T}^{n-1} \cap u\mathbb{T}^{n-1}$ is not empty.
b) If this intersection is transverse, it contains at least 2^{n-1} points.

The assumption in *b*) means that, for all $p \in \mathbb{T}^{n-1} \cap u\mathbb{T}^{n-1}$, the tangent spaces at p intersect transversally, that is $T_p\mathbb{T}^{n-1} \cap T_p\, u\mathbb{T}^{n-1} = \{0\}$.

This Fact is due to Biran, Entov and Polterovich in [13] and to Cheol-Hyun Cho in [17]. 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 $U(n)$.

Remark 3.2. When $m = 2$, Fact 3.1 is easy because $\mathbb{CP}^1$ is a round sphere and Clifford tori are great circles. Hence two of them intersect in two points. Note that the conclusion would not be true for smaller circles on the sphere. A simple explanation in this case would be that these great circles separate the sphere in two pieces of equal area. Hence one such pieces can not be strictly included into another.

Even when $m = 3$, Fact 3.1 does not seem to have a proof that does not use symplectic geometry.

Idel and Wolf reformulated Fact 3.1.a 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 $v_0 = (1, \ldots, 1)$. 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 $D := \{\mathrm{diag}(u_1, \ldots, u_n) \in U\}$.

Corollary 3.3. *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 $i = 1, \ldots, n$. Note that this decomposition is not *unique modulo the center of U*. See in [25]and also [2] for some examples.

3.2 Existence of biunimodular functions

Theorem 3.4. *Let $p \geqslant 11$ be prime. There exist biunimodular functions on $\mathbb{F}_p$ which are proportional neither to gaussian nor to Björck functions.*

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

$$T := \{[f] \in \mathbb{P}(V) \mid \ |f(x)| = |f(0)| \text{ for all } x \in \mathbb{F}_p\} \simeq \mathbb{T}^{p-1}. \qquad (3.1)$$

and $F : f \mapsto \widehat{f}$ be the Fourier transform.

Strategy of proof of Theorem 3.4. We will apply Fact 3.1.b to the unitary transformation F and the torus T. The $(p-1)p$ gaussian functions $g_{a,\ell}$ and the $4p^2$ functions $h_{\varepsilon,j,k}$ and $\overline{h}_{\varepsilon,j,k}$ introduced in Section 2.2 belong to the intersection $T \cap F^{-1}T$.

Assume, by contradiction that the intersection $T \cap F^{-1}T$ contains only gaussian and björckian functions. One can check that the intersection is transverse at all these points. Therefore Fact 3.1 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. □

3.3 Transversality of tori at gaussian functions

In order to end the proof of Theorems 3.4 we need to check the transversality of an intersection $T \cap F^{-1}T$ of suitable Clifford tori at various points: at the gaussian functions, at the björckian functions. We will only present the calculation at one gaussian function. The other calculation are also quite interesting but I do not have time for them.

Proposition 3.5. *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 3.5 when $p \equiv 1$ mod 4. In this case the Fourier transformof g_0 is given by,

$$\widehat{g}_0(2x) = \overline{g_0}(x) \text{ for all } x \text{ in } \mathbb{F}_p.$$

First step We describe the various tangent spaces.

We use the 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

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

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

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

The linear condition defining the tangent space of T at the point $[g_0]$ is

$$\mathrm{Re}(\varphi) = 0. \tag{3.2}$$

If one writes in our coordinate system

$$\widehat{g}_\varphi = \big(\mathbf{1}_{\mathbb{F}_p} + U\varphi\big)\, \widehat{g}_0,$$

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

$$\mathrm{Re}(U\varphi) \text{ is constant on } \mathbb{F}_p, \tag{3.3}$$

and one easily computes this function $U\varphi$, for all x in $\mathbb{F}_p$,

$$\begin{aligned} U\varphi(-2x) &= g_0(x) \textstyle\sum_{y\in\mathbb{F}_p} e^{-4i\pi xy/p} e^{2i\pi y^2/p} \varphi(y) \\ &= \textstyle\sum_{y\in\mathbb{F}_p} g_0(x-y)\,\varphi(y) \;\; = \;\; (g_0 * \varphi)(x). \end{aligned}$$

Second step 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 (3.2) one can write $\varphi = i\psi$ with ψ real valued. Equation (3.3) can be rewritten as

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

where $\beta_0(x) := \sin(2\pi x^2/p)$, or equivalently,

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

Since the function $\widehat{\beta}_0(2x) = -\beta_0(x)$ 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. □

Exercise 3.6. Prove Proposition 3.5 for a prime $p \equiv 3 \bmod 4$.
Indication: the proof is similar except that in that case, the Fourier transform is $\widehat{g}_0(2x) = i\,\overline{g_0}(x)$ for all x in $\mathbb{F}_p$.

Exercise 3.7. For $d \geqslant 3$ odd. Prove that there exists a function f on $\mathbb{Z}/d\mathbb{Z}$ such that $|f(0)| = |\widehat{f}(0)| = 1$ and $|f(\ell)| = |\widehat{f}(\ell)| = \frac{1}{\sqrt{2}}$, for all $\ell \neq 0$.
Indication: Choose f even: the set $\{\delta_0, \frac{1}{\sqrt{2}}(\delta_\ell + \delta_{-\ell})_{1\leqslant \ell < d/2}\}$ is an orthogonal basis of the space $V_+ := \{f : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C} \mid f(-\ell) = f(\ell)\}$ of even functions.

3.4 Finiteness of odd-biunimodular functions

In this section we introduce the biunimodular functions. Those are functions that are analogous to the biunimodular functions except that one requires that they vanish at 0. The main examples are the Dirichlet characters when $d = p$ is prime. We will particularly focus on the odd-biunimodular functions. We will see that they satisfy the same finiteness and counting result as the biunimodular functions.

Let d be an odd integer. We recall that a function f on C_d is odd if $f(-k) = -f(k)$ for all k in C_d. Note that, one has $f(0) = 0$

Definition. *Let $f : C_d \to \mathbb{C}$ be a function. We say that*
f is unimodular on $C_d \smallsetminus \{0\}$ if $f(0)=0$ and $|f(\ell)|=1$ for $\ell \neq 0$:
f is biunimodular on $C_d \smallsetminus \{0\}$ if both f and $\widehat{f}$ are unimodular on $C_d \smallsetminus \{0\}$.
f is odd-biunimodular if f is odd and is biunimodular on $C_d \smallsetminus \{0\}$.
f is a $\mathcal{C}$-function if $f^{-1}(0) = \{0\}$ and

$$\sum_{k \in C_d \smallsetminus \{0\}} f(k+\ell)\, f(k)^{-1} \;=\; -1 \quad \textit{for } \ell \neq 0. \tag{3.4}$$

We say that a $\mathcal{C}$-function is normalized if $f(1) = 1$.

As in Lemma 2.4, one can check that an odd-unimodular function is an odd-biunimodular function if and only if it is a $\mathcal{C}$-function.

Example 3.8. Let $d = p$ be a prime number. Every non trivial odd Dirichlet character χ on $\mathbb{F}_p$ is an odd-biunimodular function, and there are exactly $\frac{p-1}{2}$ odd Dirichlet characters. See Section 1.4.

Proposition 3.9. *When $d = p$ is prime, the number of normalized $\mathcal{C}$-functions is finite.*

Proof. This fact is due to Biro in 1999 in [15]. It can be proven in the same way as in Theorem 2.8. Indeed the map Φ in (2.6) is still proper as a map $E_{\geqslant 1} \times E_{\geqslant 1} \to E \times E$, where $E_{\geqslant 1} := \{f \in E \mid \|f\| \geqslant 1\}$. □

For odd functions we can compute this number.

Proposition 3.10. *When $d = p$ is prime, the number of normalized odd $\mathcal{C}$-functions counted with multiplicity is equal to $\binom{2n-2}{n-1}$ with $n = \frac{p-1}{2}$.*

Proof. We use the same argument as in Theorem 2.17. Hence we use an analogue of the proper map Φ in (2.6) between spaces of the same dimension. We introduce the vector spaces $E^{\pm} = \{f : \mathbb{F}_p \mid f(-k) = \pm f(k) \text{ for all } k\}$ and and the affine spaces $E_1^- := \{f \in E^- \mid f(1) = 1\}$. We also introduce the affine space

$$F_1^+ := \{(f_0, g_0) \in E^+ \times E^+ \mid \begin{array}{l} f_0(0) = g_0(0) = 0 \;, f_0(1) = 1 \\ \text{and } \sum\limits_{x \in \mathbb{F}_p} f_0(x) = \sum\limits_{x \in \mathbb{F}_p} g_0(x) \;\} \end{array} \Bigg\}$$

so that $\dim(F_1^+) = 2\dim(E_1^-) = 2n-2$. The new proper map Φ is

$$\Phi : E_1^- \times E_1^- \longrightarrow F_1^+ \; ; \;\; (f, g) \mapsto (f\,\check{g}, \widehat{f}\,\widehat{g}).$$

The number of points counted with multiplicity in the fibers of Φ is constant. We do the counting in the fiber $\Phi^{-1}(E_1, E_1)$ where $E_1 = \delta_1 - \delta_{-1}$ instead of $\Phi^{-1}(\mathbf{1}_{\mathbb{F}_p^*}, \mathbf{1}_{\mathbb{F}_p^*})$. With this modification the argument is as in Lemma 2.19. $\square$

Remark 3.11. It would be nice to have a counting formula for all $\mathcal{C}$-functions f on $\mathbb{F}_p$ with $f(1) = 1$, similar to the counting of $\mathcal{H}$-functions or to the counting of odd $\mathcal{C}$-functions. The argument in Proposition 3.10 does not apply to this situation because the space of functions on $\mathbb{F}_p$ that vanish at 0 is not invariant by Fourier transform.

3.5 Existence of odd-biunimodular functions

The application of Fact 3.1 to the existence of new biunimodular functions on $\mathbb{F}_p$ in Theorem 3.4 involved quite a few calculations, because one needed to check the transversality condition. In this section, we explain an application of Fact 3.1 that involves no calculation.

When d is an odd integer which is not prime, it is not so easy to construct odd biunimodular functions. The following proposition says that they always exist.

Proposition 3.12. *Let $d \geqslant 3$ be an odd integer. Then there exist odd biunimodular functions on the cyclic group C_d.*

The first non trivial case is when $d = 9$. One can prove that there are exactly 18 odd $\mathcal{C}$-functions on C_9. All of them are Galois conjugate. This explain why they are not so easy to detect. Among them 12 are biunimodular.

Proof of Proposition 3.12. 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 $T_- = \mathbb{T}^{n-1}$ of $\mathbb{P}(V_-) = \mathbb{CP}^{n-1}$ are precisely the lines spanned by odd-unimodular functions on $C_d \smallsetminus \{0\}$. Fact 3.1.a tells us that $T_- \cap F(T_-) \neq \varnothing$. This exactly means that there exists a unimodular odd $\mathcal{C}$-function. $\square$

Exercise 3.13. **Invariant odd biunimodular functions** Let p be a prime number with $p \equiv 1 \bmod 3$, let $d = p^2$ and $A = \mathbb{Z}/d\mathbb{Z}$.
a) Prove that the multiplicative group $G := (\mathbb{Z}/d\mathbb{Z})^*$ has order $(p-1)p$.
b) Prove that G is cyclic.
c) Prove that G contains a unique subgroup H of order 3.
d) Prove that $H' := H \cup -H$ is a subgroup of G of order 6.
e) Let $V' = \{f : A \to \mathbb{C} \mid f \text{ is odd and } H\text{-invariant}\}$. Compute $\dim(V')$.
f) Prove that V' is invariant by the Fourier transform F.
g) Prove that there exist H-invariant odd biunimodular functions on A.

3.6 Transversality of tori at Dirichlet characters

When $d = p$ is prime, Proposition 3.12 is not useful since we already know that the odd Dirichlet characters are odd-biunimodular. The aim of this section is to deal with this case and to prove the following theorem which answers a question raised by Harvey Cohn in 94.

Theorem 3.14. *For every prime $p \geqslant 11$, there exist odd-biunimodular functions on $\mathbb{F}_p$ that are not proportional to odd Dirichlet characters.*

This theorem is analogous to Theorem 3.4 and its proof also relies on Fact 3.1. Therefore we need to study the transversality of the intersection of the Clifford tori $T_- \cap F^{-1}T_-$ at the odd Dirichlet character. We will only present the proof when $p \equiv 1 \bmod 8$ because this case already contains many interesting ideas of the proof.

This assumption prevents the existence of odd Dirichlet characters of order 2 or 4. At these characters, the intersection is not transverse and one needs to deal with the multiplicity of this intersection by using ideas from Complex Analysis. This special case would take too much time for a graduate course.

Proposition 3.15. *Let χ be an odd Dirichlet character of $\mathbb{F}_p$.*
a) *The intersection $T_- \cap F^{-1}T_-$ is transverse at $[\chi]$ if and only if, for all non trivial even Dirichlet character ψ of $\mathbb{F}_p$, the following Jacobi sums differ*

$$J(\chi, \psi) \neq J(\overline{\chi}, \psi). \tag{3.5}$$

b) *This is always the case when $p \equiv 1$ mod 8.*

We recall from Section 1.4 that the Jacobi sum is defined as

$$J(\chi, \psi) = \sum_{x \in \mathbb{F}_p} \chi(x)\, \psi(1-x).$$

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

Proof of Theorem 3.14 when $p \equiv 1$ *mod* 8. We will apply Fact 3.1.b to the unitary transformation F and the torus T_-. The $\frac{p-1}{2}$ odd Dirichlet characters $[\chi]$ belong to the intersection $T_- \cap F^{-1}T_-$ and, according to Proposition 3.15, the intersection at these points is transverse. These points $[\chi]$ cannot be the only points of intersection because the number predicted by Fact 3.1.b is $2^{\frac{p-3}{2}}$ and, since $p \geqslant 11$, this number is larger than $\frac{p-1}{2}$. □

Proof of Proposition 3.15.a. Remember that $\dim_{\mathbb{C}} V_- = (p-1)/2$.

First step We first describe the various tangent spaces.
Let χ be an odd Dirichlet character on $\mathbb{F}_p$. Let $B_o = \{\psi_0\} \cup B'_o$ be the set of even Dirichlet characters of $\mathbb{F}_p$, ψ_0 being the trivial one and B'_o the others. We will use the following complex coordinates system $\mathbf{a} = (\mathbf{a}_\psi)_{\psi \in B'_o}$ of $\mathbb{P}(V)$ in the neighborhood of $[\chi]$. It is given by

$$\mathbf{a} \mapsto [f_{\mathbf{a}}] \;\text{ where }\; f_{\mathbf{a}} = \left(\psi_0 + \textstyle\sum_{\psi \in B'_o} \mathbf{a}_\psi \psi\right) \chi\,. \tag{3.6}$$

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

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

The linear equations defining the tangent space of T_- 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 (3.6), this can be rewritten as

$$\mathrm{Re}(\textstyle\sum_{\psi \in B'_0} \mathbf{a}_\psi(\psi - \psi_0)) \;=\; 0. \tag{3.7}$$

Since the set B'_o is invariant by complex conjugation, Condition (3.7) 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 B_o, this gives

$$T_{[\chi]}T_- \ \simeq \ \{(\mathbf{a}_\psi) \in \mathbb{C}^{B'_o} \mid \overline{\mathbf{a}_{\overline{\psi}}} = -\mathbf{a}_\psi \ \text{ for all } \psi \in B'_o\}. \tag{3.8}$$

Using Proposition 1.18, one also computes in our coordinate system

$$\begin{aligned} \widehat{f}_{\mathbf{a}} \ &= \ \tfrac{G(\chi)}{\sqrt{p}} \left(\psi_0 + \textstyle\sum_{\psi\in B'_o} \alpha_\psi \mathbf{a}_\psi \overline{\psi}\right) \overline{\chi} \ \text{ where} \\ \alpha_\psi \ &:= \ \frac{G(\chi\psi)}{G(\chi)} \ = \ \frac{G(\psi)}{J(\chi,\psi)} \ . \end{aligned} \tag{3.9}$$

One deduces from (3.8) the equality

$$T_{[\chi]}F^{-1}T_- \ \simeq \ \{(\mathbf{a}_\psi) \in \mathbb{C}^{B'_o} \mid \overline{\alpha_{\overline{\psi}}}\, \overline{\mathbf{a}_{\overline{\psi}}} = -\alpha_\psi \, \mathbf{a}_\psi \text{ for all } \psi \in B'_o\}. \tag{3.10}$$

Second step We give the transversality criterion for the tangent spaces. Since ψ is even, one has

$$\overline{\alpha_{\overline{\psi}}} \ = \ \frac{\overline{G(\overline{\psi})}}{\overline{J(\chi,\overline{\psi})}} \ = \ \frac{G(\psi)}{J(\overline{\chi},\psi)} \ . \tag{3.11}$$

Comparing (3.8) and (3.10), and using the values (3.9) and (3.11) for α_ψ and $\overline{\alpha_{\overline{\psi}}}$, one gets the equivalences:

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

This ends the proof of Proposition 3.15.a □

Remark 3.16. Note that when $p \equiv 3 \bmod 4$, the Legendre character $\chi = \chi_0$ is odd. This character satisfies $\overline{\chi}_0 = \chi_0$. Therefore the intersection $T_- \cap F^{-1}T_-$ is not transverse at $[\chi_0]$.

3.7 Using the Stickelberger's formula

We will need the following elementary formula that was already known to Kummer. This formula is the first non trivial case of the Stickelberger's formula that can be found in [32, Chap.1] or in [26, Chap.14].

Lemma 3.17. *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* $J_{j,k} := \sum\limits_{x \neq 0,1} x^{-j}(1-x)^{-k} \in \mathbb{F}_p$.

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 3.17. This is a classical and elementary calculation

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

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

We can now give the proof of Proposition 3.15.*b*

Notation We want to prove that

$$J(\chi, \psi) \neq J(\overline{\chi}, \psi) \tag{3.12}$$

by reducing it modulo a suitable prime ideal $\mathfrak{p}$ of the ring $\mathbb{Z}[\zeta_{p-1}]$. Since the multiplicative group $\mathbb{F}_p^*$ is a cyclic group of order $c := p-1$, we can introduce the smallest positive integer g_0 whose image modulo p is a generator of $\mathbb{F}_p^*$. 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 and ψ are not trivial, there exist positive integers $j, k < p-1$ such that

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

Note that j is odd while k is even.

Proof of Proposition 3.15.b. The action of an element of the Galois group of $K/\mathbb{Q}$ commutes with the complex conjugation and hence preserves the assertion (3.12). This action is given by an element $a \in (\mathbb{Z}/(p–1)\mathbb{Z})^*$ 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 3.18, we can assume that

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

The Jacobi sum $J(\chi,\psi)$ 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 roots 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 $\mathfrak{p} := (p, g_0 - \zeta_{p-1})$ 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 3.17, one has the equalities

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

since $j{+}k < p{-}1$. Similarly, one has the equalities

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

since $j < k$. This proves our assertion □

In the proof of Proposition 3.15.*b*, we used the following combinatorial lemma with $c = p{-}1$.

Lemma 3.18. *Let c be a positive integer with $c \equiv 0$ mod 8, let j be an odd integer and $k < c$ be an even positive integer. Then there exist positive integers $a, j', k' < c$ such that a is coprime to c and*

$$j' \equiv \pm aj \bmod c, \qquad k' \equiv ak \bmod c, \qquad j' \leqslant k' \leqslant c - j'. \tag{3.13}$$

Proof of Lemma 3.18. **First step** Preliminary reductions

(*i*) We can assume that $c = jr$ with r integer $r \geqslant 8$. Indeed there exists an integer x coprime to c such that $xj \equiv j'$ mod c and j' is a positive divisor of c so that $c = j'r$. Since j is odd, one has $r \equiv 0$ mod 8.

(*ii*) 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

$$j_0 := j/m,\ k_0 := k/m \text{ and } c_0 := c/m.$$

We find a pair (j_0', k_0') satisfying (3.13) with j_0, k_0, c_0. Then the pair

$$(j', k') := (mj_0', mk_0')$$

satisfies (3.13) with j, k, c.

(iii) We can assume that $k < j$. Indeed if $k > c - j$, we replace the pair (j, k) by

$$(j', k') := (j, c - k) \equiv (-aj, ak) \bmod c \text{ with} a = -1.$$

Second step Finding a, j' and k'.
We choose a prime divisor $p \geqslant 3$ of j and we write $c = pq$.

(iv) We will choose a among the integers $a_\ell := 1 + \ell q$ with $0 \leqslant \ell < p$. Indeed all of them except at most one are coprime to c.

(v) We will choose $j' = j$ because for all ℓ one has $j \equiv a_\ell j \bmod c$.

(vi) We will choose k' in the set S of integers of the form

$$S := \{k' = k + mq \mid 0 \leqslant m < p\}.$$

Since $p \geqslant 3$ and $j \leqslant r/8$, the interval $[j, c-j]$ contains at least two integers of S. By (ii), the integer k is coprime to p, therefore the integers $a_\ell k = k + \ell kq$ are distinct mod c. Therefore S is also the set of integers $k'_\ell = k + m_\ell q$ with $0 \leqslant m_\ell < p$, such that $k'_\ell \equiv a_\ell k \bmod c$. Hence by (iv), one can find a_ℓ prime to c such that $j < k'_\ell < c - j$. □

Notes to Chapter 3 The finiteness and the existence result of this chapter is in [11]. It relies on the Floer homology results in [13], [17]. See also [25].

Part II
Convolution and square

In the next four lectures, we will deal with another family of functions f on $\mathbb{Z}/d\mathbb{Z}$ called λ-critical that have properties analogous both to the gaussian functions.

Their rescaled convolution square is proportional to their square. More precisely they satisfy $f * f(2x) = \lambda f^2(x)$. For the gaussian functions the critical value λ is equal to $\pm\sqrt{d}$ when $d \equiv 1 \bmod 4$ and is equal to $\pm i\sqrt{d}$ when $d \equiv 3 \bmod 4$. Here d will be an odd integer, not necessarily prime.

The Dirichlet characters with primitive square also satisfy this equation, the corresponding critical value is given by Jacobi sums.

The main question is then what are the possible critical values λ and how can one construct the corresponding λ-critical function f.

In Lecture 4, we will introduce the Jacobi theta functions. These functions are interesting in their own and we will recall their main properties: the addition formula, the isogeny formula and the transformation formula. They are very useful since they give the embeddings of elliptic curves in projective spaces. They also give embeddings of the modular curves, i.e. the moduli space of elliptic curves They also have astonishing arithmetic properties that are part of the so-called Kronecker youth dream and that are nowadays encoded in the Shimura reciprocity.

In Lecture 5 we explain how these Jacobi theta functions restricted to a cyclic group of torsion points on the corresponding elliptic curve gives rise to λ-critical functions with $\lambda = \lambda_0 := \sqrt{a} + i\sqrt{b}$, where a and b are positive integers with $a + b = d$. The proof uses the three formulas for theta functions that we proved in the Lecture. The elliptic curve has to be chosen with care. In particular, it has complex multiplication by $i\sqrt{ab}$. The integers a and b have to satisfy congruence conditions modulo 4 that can entirely be explained by the transformation formula. Moreover the sign in the transformation formula explains that λ_0 is always critical but $-\lambda_0$ is sometimes not critical.

In the next two lectures, we extend the results of the previous two lectures to higher dimension.

In Lecture 6 we introduce the abelian varieties that will replace the elliptic curves. An important point of the discussion is that very few higher dimensional complex tori are abelian varieties. The abelian varieties are those that admit an integral Kähler structure. They are parametrized by the Riemann matrices τ. These matrices live in the Siegel upper half-space $\mathcal{H}_g$ that will replace Poincaré upper half-plane. The symplectic group $\mathrm{Sp}(g, \mathbb{R})$ which is the group of isometries of $\mathcal{H}_g$ will replace the group $\mathrm{SL}(2, \mathbb{R})$. The abelian varieties that will give rise to critical values are those that admit non-trivial unitary $\mathbb{Q}$-endomorphisms.

In Lecture 7 we introduce the Riemann theta functions: they generalize the Jacobi theta functions and still satisfy the addition formula, the isogeny formula and the transformation formula. We give the interpretation as section of line bundle on the abelian variety and on the moduli space $\mathcal{A}_g$ of polarized abelian variety. We explain how one can choose these Riemann theta functions such that their restriction to a suitable cyclic group of torsion points on the corresponding abelian variety give rise to λ-critical functions for values λ like $\lambda = 1 + \sqrt{5} + i\sqrt{9 - 2\sqrt{5}}$ when $d = 15$ or like $\lambda = 1 + 2\sqrt{2} + 2i\sqrt{3 - \sqrt{2}}$ when $d = 21$.

4 Jacobi theta functions

The aim of this lecture is to introduce the Jacobi theta functions $\theta(z, \tau)$ and to explain why they are useful.

As a function of z, we interpret them as section of a line bundle on an elliptic curve E_τ and we prove the addition formula together with the isogeny formula.

As a function of τ we prove the modularity properties of the function θ with a cautious care in the sign that occurs in the transformation formula.

We also explain the Riemann theta relations that allow to embed both the elliptic curves E_τ and the modular curves $X(m)$ in projective spaces. We just give one example for each of these embeddings.

4.1 Line bundles on elliptic curve

Theta functions will occur naturally as sections of line bundles over an elliptic curve. As a complex analytic curve, an elliptic curve is a quotient $E = \mathbb{C}/\Lambda$ of the complex plane $\mathbb{C}$ by a lattice Λ. One will write this lattice under the form $\Lambda = \Lambda_\tau := \mathbb{Z}\tau \oplus \mathbb{Z}$ where the parameter τ belongs to the upper half plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$. This is not restrictive since for every $\alpha \in \mathbb{C}^*$ the lattice Λ and $\alpha\Lambda$ gives rise to the same curve. We write $E_\tau := E/\Lambda_\tau$.

For $d \in \mathbb{Z}$ we consider the space of quasiperiodic holomorphic functions

$$V_d(\tau) = \{f \in \mathrm{Hol}(\mathbb{C}) \mid f(z+1) = f(z) \text{ and } f(z+\tau) = e^{-i\pi d\tau} e^{-2i\pi dz} f(z)\}$$

In this definition the factor $e^{-i\pi d\tau}$ is not so important. It is useful, because for $d \geqslant 1$ this space contains the d^{th}-power $\theta(z, \tau)^d$ of the Jacobi theta function that we define now.

As a function of z, the Jacobi theta function is roughly defined as a "Fourier series whose Fourier coefficients are gaussian". More precisely,

$$\theta_\tau(z) = \theta(z, \tau) := \sum_{m \in \mathbb{Z}} e^{i\pi\tau m^2} e^{2i\pi mz}, \text{ for } z \in \mathbb{C} \text{ and } \tau \in \mathbb{H}. \tag{4.1}$$

Note that the condition $\tau \in \mathbb{H}$ is the one needed for the convergence of this series. This function belongs to $V_1(\tau)$ since one has

$$\theta_\tau(z+1) = \theta_\tau(z) \text{ and } \theta_\tau(z+\tau) = e^{-i\pi\tau} e^{-2i\pi z} \theta_\tau(z)\,. \tag{4.2}$$

And, for $d \geqslant 1$, its power θ_τ^d belong to $V_d(\tau)$.

It is important to know exactly where the zeros of the functions θ_τ are.

Lemma 4.1. *a) The function θ_τ is even: one has $\theta_\tau(-z) = \theta_\tau(z)$.*
b) One has $\theta_\tau(\frac{\tau+1}{2}) = 0$.
c) Conversely, if $\theta_\tau(z) = 0$, then one has $z = \frac{\tau+1}{2} + m\tau + n$ with m, n in $\mathbb{Z}$.

Proof. *a*) This follows from Formula (4.1).

b) One computes using (4.2) and *a*), $\theta_\tau(\tau{+}1{-}z) = e^{-i\pi\tau}e^{2i\pi z}\,\theta_\tau(z)$, one evaluates this equality at $z = \frac{\tau+1}{2}$, and one gets $\theta_\tau(\frac{\tau+1}{2}) = -\theta_\tau(\frac{\tau+1}{2})$.

c) One checks that the parallelogram P with vertices 0, 1, τ+1, τ contains only one zero of the function θ_τ by computing the number N of zeros as an integral $N = \frac{1}{2i\pi}\int_{\partial P}\frac{\theta_\tau'(z)}{\theta_\tau(z)}\,\mathrm{d}z$. The quasiperiodicity of θ_τ in (4.2), allows simplification in the integration on the opposite sides of the parallelogram ∂P and one gets $N = \frac{1}{2i\pi}\int_0^1(2i\pi)\,\mathrm{d}z = 1$. □

Lemma 4.2. *a) For $d \geqslant 1$, the dimension of the space V_d is d.*
b) For $d \leqslant -1$, one has $V_d = \{0\}$.

Remark 4.3. When $d = 0$ a function in $V_d(\tau)$ is a bounded holomorphic function, hence it is constant.

Proof. Let $f \in V_d(\tau)$. We write $z = x + iy$, with x and y real. Since f is periodic it has a Fourier expansion that we choose to write as

$$f(z) = \sum_{n\in\mathbb{Z}} a_n\, e^{i\pi n^2\tau/d}\, e^{2i\pi nz}. \tag{4.3}$$

A priori the Fourier coefficient $a_n = a_n(y)$ might depend on y. But, since f is holomorphic, one has $\overline{\partial}_z a_n = 0$, and it does not. We have chosen to express f that way so that the quasiperiodicity condition on f can be expressed in a very simple way: $a_{n+d} = a_n$ for all $n \in \mathbb{Z}$. The sequence a_n has period $|d|$. Since the series (4.3) converges, and since $Im(\tau) > 0$, one must have $d \geqslant 1$. Conversely, when $d \geqslant 1$ these series converges and f is known as soon as one knows the coefficients $a_0, \ldots, a_{d-1}$. This proves that the space $V_d(\tau)$ has dimension d. □

4.2 Theta functions with characteristic

There are different notations and more precisely different normalizations for the theta functions, depending on the applications one has in mind. The following one is the most usual.

The *classical theta functions with characteristic* a, b in $\mathbb{C}$, are defined by, for $z \in \mathbb{C}$ and $\tau \in \mathbb{H}$,

$$\begin{aligned} \theta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau) &:= \sum_{m\in\mathbb{Z}} e^{i\pi(m+a)^2\tau} e^{2i\pi(m+a)(z+b)}. \\ &= e^{i\pi a^2\tau} e^{2i\pi a(z+b)}\, \theta(z + a\tau + b, \tau). \end{aligned}$$

Forgetting the exponential factors, one may think of the parameter a as a translation in the direction of the period 1 and of the parameter b as a translation in the direction of the quasiperiod τ. This is geometrically correct at least when a and b are real.

One has to be careful that these functions do not belong to $V_1(\tau)$ except when a and b are integers, indeed, one has

$$\begin{aligned} \theta\begin{bmatrix} a \\ b \end{bmatrix}(z+1,\tau) &= e^{2i\pi a}\, \theta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau) \quad \text{and} \\ \theta\begin{bmatrix} a \\ b \end{bmatrix}(z+\tau,\tau) &= e^{-i\pi\tau} e^{-2i\pi(z+b)}\, \theta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau). \end{aligned}$$

Note that these functions depend only on $b + z$, hence it is not restrictive to study them when $b = 0$ and to define

$$\theta_\tau\begin{bmatrix} a \\ z \end{bmatrix} := \theta\begin{bmatrix} a \\ 0 \end{bmatrix}(z,\tau) = \theta\begin{bmatrix} a \\ z \end{bmatrix}(0,\tau) \tag{4.4}$$

Note that these functions satisfy the following periodicity when translating the characteristic by elements m, n in $\mathbb{Z}$,

$$\theta\begin{bmatrix} a+m \\ b+n \end{bmatrix}(z,\tau) = e^{2i\pi an}\, \theta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau). \tag{4.5}$$

It follows from the proof of Lemma 4.2

Lemma 4.4. *The functions* $z \mapsto \theta\begin{bmatrix} k/d \\ 0 \end{bmatrix}(dz, d\tau)$, *with* $k = 0, \ldots, d-1$ *form a basis of the vector space* $V_d(\tau)$.

We will mainly use the following theta functions with characteristics. For $\xi \in \mathbb{Z}^g/2\mathbb{Z}^g$, seen as a subset of $\mathbb{Z}^g$, we define

$$\theta_{[0]}(z,\tau) = \theta\begin{bmatrix} 0 \\ 0 \end{bmatrix}(2z, 2\tau) := \sum_{m \text{ even}} e^{i\pi m^2\tau/2} e^{2i\pi mz}. \tag{4.6}$$

$$\theta_{[1]}(z,\tau) = \theta\begin{bmatrix} 1/2 \\ 0 \end{bmatrix}(2z, 2\tau) := \sum_{m \text{ odd}} e^{i\pi m^2\tau/2} e^{2i\pi mz}. \tag{4.7}$$

Note that one has the equalities:

$$\theta_{[0]}(z,\tau) = \theta(2z, 2\tau) \quad \text{and} \quad \theta_{[0]}(z,\tau) + \theta_{[1]}(z,\tau) = \theta(z, \tau/2). \tag{4.8}$$

4.3 The addition and the isogeny formula

We want to explain two classical formulas for the theta functions, the "addition formula" and the "isogeny formula". We will only need special cases of these formulas that we state below.

The first formula that we need will be a corollary of the following addition formula.

Lemma 4.5. Addition formula *For all a, b, z, w in $\mathbb{C}$, $\tau \in \mathbb{H}$, one has*

$$\theta_\tau\begin{bmatrix} a+b \\ z+w \end{bmatrix}\theta_\tau\begin{bmatrix} a-b \\ z-w \end{bmatrix} \;=\; \theta_{2\tau}\begin{bmatrix} a \\ 2z \end{bmatrix}\theta_{2\tau}\begin{bmatrix} b \\ 2w \end{bmatrix} \;+\; \theta_{2\tau}\begin{bmatrix} a+\frac{1}{2} \\ 2z \end{bmatrix}\theta_{2\tau}\begin{bmatrix} b+\frac{1}{2} \\ 2w \end{bmatrix}. \qquad (4.9)$$

Proof. Just write the left-hand side as a double sum over m, n in $\mathbb{Z}$ and write $m = (p+\varepsilon) + (q+\varepsilon)$ and $n = (p+\varepsilon) - (q+\varepsilon)$ where p and q are in $\mathbb{Z}$ and where $\varepsilon = 0$ or $\frac{1}{2}$ according to the parity of $m-n$. This gives

$$\begin{aligned} LHS &= \sum_{m,n} e^{i\pi(m+a+b)^2\tau} e^{2i\pi(m+a+b)(z+w)} e^{i\pi(n+a-b)^2\tau} e^{2i\pi(n+a-b)(z-w)}, \\ &= \sum_{\varepsilon,p,q} e^{2i\pi(p+a+\varepsilon)^2\tau} e^{4i\pi(p+a+\varepsilon)z} e^{2i\pi(q+b+\varepsilon)^2\tau} e^{4i\pi(q+b+\varepsilon)w} \\ &= \sum_{\varepsilon} \theta_{2\tau}\begin{bmatrix} a+\varepsilon \\ 2z \end{bmatrix}\theta_{2\tau}\begin{bmatrix} b+\varepsilon \\ 2w \end{bmatrix}, \end{aligned}$$

where the sum has two terms $\varepsilon = 0$ or $1/2$. □

When $a = b = 0$, one gets the following corollary.

Corollary 4.6. *For all z, w in $\mathbb{C}$, $\tau \in \mathbb{H}$, one has*

$$\theta(z+w,\tau)\theta(z-w,\tau) \;=\; \theta_{[0]}(w,\tau)\theta_{[0]}(z,\tau) + \theta_{[1]}(w,\tau)\theta_{[1]}(z,\tau). \qquad (4.10)$$

Note that this formula is not surprising because one can check easily that, as a function of z, the left-hand side belongs to the space 2-dimensional space $V_2(\tau)$. Hence it is a linear combination of the two functions $\theta_{[0]}$ and $\theta_{[1]}$ that form a basis of $V_2(\tau)$.

Here is the second formula which is simple but useful.

Lemma 4.7. Isogeny formula *For $\tau \in \mathbb{H}$, d positive integer, one has*

$$\sum_{\ell\in\mathbb{Z}/d\mathbb{Z}} \theta(\ell/d,\tau) = d\,\theta(0, d^2\tau).$$

Proof. Just write the left-hand sides as a double sum

$$\sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} \theta(\ell/d, \tau) \;=\; \sum_m e^{i\pi m^2 \tau} \sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} e^{2i\pi m\ell/d} \;=\; d \sum_n e^{i\pi n^2 d^2 \tau} \;=\; d\,\theta(0, d^2\tau)$$

where we used the fact that $\sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} e^{2i\pi\ell m/d}$ is equal to d when d divides m and is equal to 0 otherwise. □

We will need the following variation of the isogeny formula for which we need d to be odd. The proof is the same.

Corollary 4.8. *For $\tau \in \mathbb{H}$, d odd positive integer, one has*

$$\sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} \theta_{[0]}(\ell/d, \tau) = d\,\theta_{[0]}(0, d^2\tau) \quad \text{and} \quad \sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} \theta_{[1]}(\ell/d, \tau) = d\,\theta_{[1]}(0, d^2\tau).$$

4.4 The transformation formula

We now explain the modularity properties of the theta functions. These properties come from a basis change in the lattice Λ that define the elliptic curve E.

These formulas deal with an element $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$. For a positive integer m we will denote by $\Gamma(m)$ the subgrooup

$$\Gamma(m) := \{\sigma \in \mathrm{SL}(2, \mathbb{Z}) \mid \sigma \equiv \pm\mathbf{1} \bmod m\}, \tag{4.11}$$

Lemma 4.9. Transformation formula *a) If $\sigma \in \Gamma(2)$, and $\gamma > 0$, then there exists a eighth root of unity $\kappa(\sigma)$ such that*

$$\theta(0, \sigma\tau) \;=\; \kappa(\sigma)\;(\gamma\tau + \delta)^{\frac{1}{2}}\;\theta(0, \tau). \tag{4.12}$$

b) The constant $\kappa(\sigma)$ is given by the formula

$$\kappa(\sigma) \;=\; i^{\frac{\delta-1}{2}} \left(\tfrac{\gamma}{\delta}\right). \tag{4.13}$$

The transformation formula with the precise determination of the constant $\kappa(\sigma)$ is due to Hecke.

Let us explain the notation in this formula.
- The $\mathrm{SL}(2, \mathbb{Z})$ action on $\mathbb{H}$ is the standard action $\sigma\tau = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$.

- For a complex number z with $Re(z) \geqslant 0$ or $Im(z) \geqslant 0$, the number $w = z^{\frac{1}{2}}$ is the unique square root with $Re(w) + Im(w) \geqslant 0$.
- The symbol $(\frac{\gamma}{\delta}) = \pm 1$ is the Jacobi symbol introduced in Section 1.3 and defined for two relatively prime integers γ and δ with δ odd.

The key ingredient is the Poisson summation formula. We recall that the Schwartz space $\mathcal{S}(\mathbb{R})$ is the space of $\mathcal{C}^\infty$ functions h on $\mathbb{R}$ all of whose derivatives decay faster than the inverse of any positive polynomial. The Fourier transform of such a function h is defined by

$$\widehat{h}(x) \ := \ \int_{\mathbb{R}} h(y) e^{2i\pi xy} \,\mathrm{d}y\,.$$

This function $\widehat{h}$ also belongs to $\mathcal{S}(\mathbb{R})$.

Fact 4.10. (Poisson summation formula) *For all $h \in \mathcal{S}(\mathbb{R})$, one has*

$$\sum_{n\in\mathbb{Z}} h(n) \ = \ \sum_{n\in\mathbb{Z}} \widehat{h}(n)\,. \tag{4.14}$$

We will also need the following elementary lemma

Lemma 4.11. *The group $\Gamma(2)$ is generated by $u^2 := \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$, $v^2 := \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ and $\pm\mathbf{1}$.*

Note that the analogous statement for $\Gamma(m)$, $m \geqslant 3$ is not true.

Proof of Lemma 4.11. We want to prove that any $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ * & * \end{smallmatrix}\right) \in \Gamma(2)$ is obtained as a product of these three matrices and their inverses. We argue by induction on the odd integer $|\alpha| + |\beta|$.

If $|\alpha| + |\beta| = 1$, one has $\sigma = \pm v^{2n}$ for some $n \in \mathbb{Z}$.

If $|\alpha| + |\beta| > 1$ and $|\alpha| < |\beta|$, for a suitable choice of sign, one has $\sigma\, u^{\pm 2} = \left(\begin{smallmatrix} \alpha & \beta' \\ * & * \end{smallmatrix}\right)$ with $\beta' = \beta \pm 2\alpha$ satisfying $|\beta'| < |\beta|$.

If $|\alpha| + |\beta| > 1$ and $|\alpha| > |\beta|$, for a suitable choice of sign, one has $\sigma\, v^{\pm 2} = \left(\begin{smallmatrix} \alpha' & \beta \\ * & * \end{smallmatrix}\right)$ with $\alpha' = \alpha \pm 2\beta$ satisfying $|\alpha'| < |\alpha|$. □

Proof of Lemma 4.9.a. It is enough to prove that

$$\theta(0, \sigma\tau)^8 \ = \ (\gamma\tau + \delta)^4\, \theta(0, \tau)^8. \tag{4.15}$$

This will prove (4.12) up to a eigth root of unity $\kappa(\sigma, \tau)$. This root will not depend on τ by a continuity argument.

We first notice that the map $(\sigma, \tau) \mapsto c(\sigma, \tau) := \gamma\tau + \delta$ is a cocycle on $\mathrm{SL}(2, \mathbb{Z}) \times \mathbb{H}$. This means that $c(\sigma_1\sigma_2, \tau) = c(\sigma_1, \sigma_2\tau)\, c(\sigma_2, \tau)$. Therefore it is enough to check (4.15) on generators of the group $\Gamma(2)$.

Let $w_0 := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $u := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Since the group $\Gamma(2)$ is generated by u^2 and $v^2 w_0 u^2 w_0^{-1}$, it is enough to check (4.12), for $\sigma = u^2$ and for $\sigma = w_0$.

The case $\sigma = u^2$ follows from the equality

$$\theta(0, \tau + 2) \;=\; \theta(0, \tau),$$

The case $\sigma = w_0$ follows from the equality

$$\theta(0, -1/\tau) \;=\; (\tau/i)^{\frac{1}{2}}\, \theta(0, \tau). \qquad (4.16)$$

which is nothing but the Poisson summation formula applied to the function $h(x) = (\tau/i)^{\frac{1}{2}}\, e^{i\pi x^2\tau}$ whose Fourier transform is $\widehat{h}(x) = e^{-i\pi x^2/\tau}$. □

4.5 The sign in the transformation formula

We now compute the eighth root of unity $\kappa(\sigma)$.

Before starting the calculation I want to make two comments that follow from a cautious examination of the previous proof.

First of all one has $\kappa(\sigma)^4 = 1$ because an element of $\Gamma(2)$ expressed as a word in u^2 and w_0 involves an even number of w_0.

Second, since $(\sigma, \tau) \mapsto \gamma\tau + \delta$ is a cocycle, the map $\Gamma \to \{\pm 1\}; \sigma \mapsto \kappa(\sigma)^2$ is a group morphism. Hence it is not difficult to check that $\kappa(\sigma)^2 = (-1)^{\frac{\delta-1}{2}}$ by checking it on the two generators u^2 and $w_0 u^2 w_0^{-1}$ of $\Gamma(2)$.

Therefore if one is only interested in the value of $\kappa(\sigma)$ up to a sign, one does not need to read the calculation below. What makes this calculation delicate is that it involves square roots of complex numbers and one has to be very precise on the choice of these square roots at each step of the calculation.

Proof of Lemma 4.9.b. The strategy is clear. The idea is to compare the asymptotic of both sides of Formula (4.12) when τ goes to 0. More precisely, we will compute the limit when τ goes to 0 of both sides of the equality

$$(\tau/i)^{\frac{1}{2}}\theta(0, \sigma\tau) \;=\; \kappa(\sigma)\; (\gamma\tau + \delta)^{\frac{1}{2}}\; (\tau/i)^{\frac{1}{2}}\theta(0, \tau). \qquad (4.17)$$

Because of the Poisson formula (4.16), the limit of the right-hand side RHS of (4.17) is

$$\lim_{\tau\to 0} RHS \ = \ \kappa(\sigma)\ \delta^{\frac{1}{2}}\ \lim_{\tau\to 0}\theta(0,-1/\tau) \ = \ \kappa(\sigma)\ \delta^{\frac{1}{2}}\,. \tag{4.18}$$

In order to compute the limit of the left-hand side LHS of (4.17) we write $\sigma\tau = \frac{\beta}{\delta}+\rho$, where $\rho := \frac{\tau/\delta}{\gamma\tau+\delta}$ is an element of $\mathbb{H}$ that also goes to 0. Taking into account that β is an even integer, one computes

$$\begin{aligned}\theta(0,\tfrac{\beta}{\delta}+\rho) \ &= \ \sum_{1\leqslant r\leqslant|\delta|}\ \sum_{m\in\mathbb{Z}} e^{i\pi(m\delta+r)^2(\frac{\beta}{\delta}+\rho)} \\ &= \ \sum_{1\leqslant r\leqslant|\delta|} e^{i\pi\frac{\beta}{\delta}r^2} \sum_{m\in\mathbb{Z}} e^{i\pi(m\delta+r)^2\rho}\,.\end{aligned}$$

We apply Poisson Formula (4.14) to the function $h(x) = \delta(\rho/i)^{\frac{1}{2}}\, e^{i\pi(\delta x+r)^2\rho}$ whose Fourier transform is $\widehat{h}(x) = e^{-i\pi\delta^{-2}x^2/\rho}e^{-2i\pi\frac{r}{\delta}x}$. Therefore we get

$$\delta(\rho/i)^{\frac{1}{2}}\theta(0,\tfrac{\beta}{\delta}+\rho) \ = \ \sum_{1\leqslant r\leqslant|\delta|} e^{i\pi\frac{\beta}{\delta}r^2} \sum_{m\in\mathbb{Z}} e^{-i\pi\delta^{-2}m^2/\rho}e^{-2i\pi\frac{r}{\delta}m}\,.$$

Therefore one has the equality

$$\lim_{\tau\to 0} LHS \ = \ \sum_{1\leqslant r\leqslant|\delta|} e^{i\pi\frac{\beta}{\delta}r^2}. \tag{4.19}$$

Remembering that both β and γ are even integers, that δ is an odd integer coprime to both of them and that $\beta\gamma \equiv -1 \mod \delta$, and comparing (4.18) and (4.19), one gets

$$\kappa(\sigma) \ = \ 1/\delta^{\frac{1}{2}} \sum_{1\leqslant r\leqslant|\delta|} e^{-i\pi\frac{\gamma}{\delta}r^2} \tag{4.20}$$

This Gauss sum can be calculated using Lemma 1.5 and Proposition 1.14.

When $\delta > 0$, one gets

$$\kappa(\sigma) = i^{\frac{(\delta-1)^2}{4}}\big(\tfrac{-2\gamma}{\delta}\big) \ = \ i^{\frac{(\delta-1)^2}{4}} i^{\delta-1} i^{\frac{1-\delta^2}{4}}\big(\tfrac{\gamma}{\delta}\big) \ = \ i^{\frac{\delta-1}{2}}\big(\tfrac{\gamma}{\delta}\big).$$

When $\delta < 0$, one gets

$$\kappa(\sigma) = i^{-1} i^{\frac{(|\delta|-1)^2}{4}}\big(\tfrac{2\gamma}{|\delta|}\big) \ = \ i^{-1} i^{\frac{(\delta+1)^2}{4}} i^{\frac{1-\delta^2}{4}}\big(\tfrac{\gamma}{\delta}\big) \ = \ i^{\frac{\delta-1}{2}}\big(\tfrac{\gamma}{\delta}\big).$$

This ends the calculation of $\kappa(\sigma)$. □

There also exists a transformation formula valid for all z. We first express it in a naive way where an exponential factor is involved.

Corollary 4.12. *If $\sigma \in \Gamma(2)$, and $\gamma > 0$, then, for all z in $\mathbb{C}$ and τ in $\mathbb{H}$,*

$$\theta(\tfrac{z}{\gamma\tau+\delta}, \sigma\tau) \;=\; i^{\frac{\delta-1}{2}} \left(\tfrac{\gamma}{\delta}\right) (\gamma\tau+\delta)^{\frac{1}{2}}\, e^{i\pi \frac{\gamma z^2}{\gamma\tau+\delta}}\, \theta(z,\tau). \tag{4.21}$$

We now express it in a simpler form by using the theta functions with characteristics. This formula is particularly simple when it is expressed with the *modified* theta function

$$\widetilde{\theta}_\tau\begin{bmatrix} a \\ b \end{bmatrix} \;=\; e^{-i\pi ab}\, \theta_\tau\begin{bmatrix} a \\ b \end{bmatrix}. \tag{4.22}$$

Note that there is no *modification* when $b = 0$.

Corollary 4.13. *Let $\tau \in \mathbb{H}$ and $\sigma \in \Gamma(2)$. Then, for a, b in $\mathbb{C}$, one has*

$$\widetilde{\theta}_{\sigma\tau}\begin{bmatrix} \delta a - \gamma b \\ -\beta a + \alpha b \end{bmatrix} \;=\; i^{\frac{\delta-1}{2}} \left(\tfrac{\gamma}{\delta}\right) (\gamma\tau+\delta)^{\frac{1}{2}}\; \widetilde{\theta}_\tau\begin{bmatrix} a \\ b \end{bmatrix}. \tag{4.23}$$

Proof. The proof of both corollaries is the same as for Lemma 4.9. We check the formula up to a eighth root of unity by checking it on the two generators of $\Gamma(2)$. The determination of this root of unity follows from a continuity argument and the case where $a = b = 0$ done in Lemma 4.9 □

We introduce now the four Jacobi theta-functions $\theta_{a,b}$ with a, b equal to 0 or 1, given by

$$\theta_{ab}(z) = \theta_{ab}(z,\tau) := \theta\begin{bmatrix} a/2 \\ b/2 \end{bmatrix}(z,\tau) = \sum_{m\in\mathbb{Z}} e^{i\pi\tau(m+\frac{a}{2})^2} e^{2i\pi(m+\frac{a}{2})(z+\frac{b}{2})} \tag{4.24}$$

Exercise 4.14. Prove the following equalities where τ is implicit.
a) $\theta_{00}(-z) = \theta_{00}(z)$, $\theta_{01}(-z) = \theta_{01}(z)$, $\theta_{10}(-z) = \theta_{10}(z)$, $\theta_{11}(-z) = -\theta_{11}(z)$.
b) Prove that $\theta_{00}(z+1) = \theta_{00}(z)$, $\theta_{01}(z+1) = \theta_{01}(z)$,
$\theta_{10}(z+1) = -\theta_{10}(z)$, $\theta_{11}(z+1) = -\theta_{11}(z)$.
c) Prove that $\theta_{00}(z+\tau) = e^{-i\pi\tau}e^{-2i\pi z}\theta_{00}(z)$, $\theta_{01}(z+\tau) = -e^{-i\pi\tau}e^{-2i\pi z}\theta_{01}(z)$,
$\theta_{10}(z+\tau) = e^{-i\pi\tau}e^{-2i\pi z}\theta_{10}(z)$, $\theta_{11}(z+\tau) = -e^{-i\pi\tau}e^{-2i\pi z}\theta_{11}(z)$.

Exercise 4.15. Prove the following equalities where $\alpha_{z,\tau} = (\tau/i)^{\frac{1}{2}} e^{i\pi z^2/\tau}$,
a) $\theta_{00}(z,\tau+1) = \theta_{01}(z,\tau)$, $\theta_{01}(z,\tau+1) = \theta_{00}(z,\tau)$,
$\theta_{10}(z,\tau+1) = e^{i\pi/4}\theta_{10}(z,\tau)$, $\theta_{11}(z,\tau+1) = e^{i\pi/4}\theta_{11}(z,\tau)$,
b) $\theta_{00}(\frac{z}{\tau}, \frac{-1}{\tau}) = \alpha_{z,\tau}\,\theta_{00}(z,\tau)$, $\theta_{01}(\frac{z}{\tau}, \frac{-1}{\tau}) = \alpha_{z,\tau}\,\theta_{10}(z,\tau)$,
$\theta_{10}(\frac{z}{\tau}, \frac{-1}{\tau}) = \alpha_{z,\tau}\,\theta_{01}(z,\tau)$, $\theta_{11}(\frac{z}{\tau}, \frac{-1}{\tau}) = -i\alpha_{z,\tau}\,\theta_{11}(z,\tau)$.

4.6 Riemann theta relations

The addition formula (4.9) relates θ functions with parameter τ with theta functions with parameter 2τ. There is another relation due to Riemann that gives a lot of quartic relations between theta functions with the same parameter τ. We begin by the general and easy to remember formulation in terms of theta function with characteristic.

Proposition 4.16. *For a, b, c, d, u, v, w, x in $\mathbb{C}$, $\tau \in \mathbb{H}$, one has $LHS = RHS$ where*

$$LHS \;=\; 2\,\theta_\tau\begin{bmatrix} \frac{a+b+c+d}{2} \\ \frac{u+v+w+x}{2}\end{bmatrix}\theta_\tau\begin{bmatrix} \frac{a+b-c-d}{2} \\ \frac{u+v-w-x}{2}\end{bmatrix}\theta_\tau\begin{bmatrix} \frac{a-b+c-d}{2} \\ \frac{u-v+w-x}{2}\end{bmatrix}\theta_\tau\begin{bmatrix} \frac{a-b-c+d}{2} \\ \frac{u-v-w+x}{2}\end{bmatrix}$$

$$RHS \;=\; \sum_{\varepsilon,\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} e^{-2i\pi(a+b+c+d)\eta}\,\theta_\tau\begin{bmatrix} a+\varepsilon \\ u+\eta\end{bmatrix}\theta_\tau\begin{bmatrix} b+\varepsilon \\ v+\eta\end{bmatrix}\theta_\tau\begin{bmatrix} c+\varepsilon \\ w+\eta\end{bmatrix}\theta_\tau\begin{bmatrix} d+\varepsilon \\ x+\eta\end{bmatrix}.$$

Proof of Proposition 4.16. The left-hand side is a sum over the lattice $\mathbb{Z}^4$ in $\mathbb{R}^4$. The idea is that the matrix $T := \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1\end{pmatrix}$ is an orthogonal matrix that sends the lattice $\mathbb{Z}^4$ to the lattice $L := T(\mathbb{Z}^4)$ which is almost $\mathbb{Z}^4$. More precisely the intersection $L_0 := L \cap \mathbb{Z}^4$ has index 2 in both L and $\mathbb{Z}^4$. Note also that $T^2 = \mathbf{1}$. We denote by A and U the column vectors $A := {}^t(a, b, c, d)$ and $U := {}^t(u, v, w, x)$. We will also need the column vector $E := {}^t(1, 1, 1, 1)$ so that

$$L_0 = \{M \in \mathbb{Z}^4 \mid {}^tEM \in 2\mathbb{Z}\} \;\text{ and }\; L = L_0 \cup (\tfrac{1}{2}E + L_0).$$

One computes,

$$LHS \;=\; 2\sum_{M\in\mathbb{Z}^4} e^{i\pi\,{}^t(M+TA)(M+TA)\tau} e^{2i\pi\,{}^t(M+TA)TU}.$$

Writing $M = T(N + \varepsilon E)$ with $\varepsilon \in \{0, \frac{1}{2}\}$, $N \in \mathbb{Z}^4$ satisfying ${}^tEN \in 2\mathbb{Z}$, one gets using the fact that T is orthogonal

$$LHS \;=\; \sum_{\varepsilon,\eta\in\{0,\frac{1}{2}\}} e^{-2i\pi\,\eta{}^tAE} \sum_{N\in\mathbb{Z}^4} e^{i\pi\,{}^t(N+A+\varepsilon E)(N+A+\varepsilon E)\tau} e^{2i\pi\,{}^t(N+A+\varepsilon E)(U+\eta E)}.$$

which is exactly RHS. In this computation, we used the fact that $\varepsilon\eta{}^tEE$ is an integer. We also used the fact that
$\sum_{\eta\in\{0,\frac{1}{2}\}} e^{2i\pi\eta\,{}^tNE} = 2$ if ${}^tEN \equiv 0$ mod 2 and $= 0$ otherwise. □

These Riemann θ relations are most often applied with $a, b, c, d \in \frac{1}{2}\mathbb{Z}$ with $a+b+c+d \in \mathbb{Z}$ so that the exponential in the RHS is a sign ± 1 and with some specialization on the variables u, v, w, x, imposing some of them to be 0 or to be equal. When $a+b+c+d \in 2\mathbb{Z}$ the sign is always $+1$. For instance, one gets the following relations between the four Jacobi theta functions θ_{ab} in (4.24). In the following formulas, the variable τ is implicit.

Corollary 4.17. *a) For y, z in $\mathbb{C}$, $\tau \in \mathbb{H}$, one has*

$$\begin{aligned}\theta_{00}(0)^2\,\theta_{00}(y+z)\,\theta_{00}(y-z) &= \theta_{00}(y)^2\,\theta_{00}(z)^2 + \theta_{11}(y)^2\,\theta_{11}(z)^2\\ &= \theta_{10}(y)^2\,\theta_{10}(z)^2 + \theta_{01}(y)^2\,\theta_{01}(z)^2.\end{aligned}$$

b) Similarly, for y, z in $\mathbb{C}$, $\tau \in \mathbb{H}$, one has

$$\begin{aligned}\theta_{00}(0)^2\,\theta_{11}(y+z)\,\theta_{11}(y-z) &= \theta_{11}(y)^2\,\theta_{00}(z)^2 - \theta_{00}(y)^2\,\theta_{11}(z)^2\\ &= \theta_{01}(y)^2\,\theta_{10}(z)^2 - \theta_{10}(y)^2\,\theta_{01}(z)^2.\end{aligned}$$

c) In particular, one has

$$\begin{aligned}\theta_{00}(0)^2\,\theta_{00}(z)^2 &= \theta_{10}(0)^2\,\theta_{10}(z)^2 + \theta_{01}(0)^2\,\theta_{01}(z)^2\\ \theta_{00}(0)^2\,\theta_{11}(z)^2 &= \theta_{10}(0)^2\,\theta_{01}(z)^2 - \theta_{01}(0)^2\,\theta_{10}(z)^2.\end{aligned}$$

d) In particular, one has $\theta_{00}(0)^4 = \theta_{01}(0)^4 + \theta_{10}(0)^4$.

Proof. a) We combine two Riemann θ relations, the first one with $a = b = c = d = 0$ and $u = v = y$, $w = x = z$ is

$$\begin{aligned}&2\theta_{00}(0)^2\,\theta_{00}(y+z)\,\theta_{00}(y-z) =\\ &\theta_{00}(y)^2\,\theta_{00}(z)^2 + \theta_{11}(y)^2\,\theta_{11}(z)^2 + \theta_{10}(y)^2\,\theta_{10}(z)^2 + \theta_{01}(y)^2\,\theta_{01}(z)^2,\end{aligned}$$

the second one with $a = 1$, $b = c = d = 0$ and $u = y+1$, $v = y$, $w = x = z$ is

$$\begin{aligned}&2\theta_{11}(0)^2\,\theta_{11}(y+z)\,\theta_{11}(y-z) =\\ &\theta_{00}(y)^2\,\theta_{00}(z)^2 + \theta_{11}(y)^2\,\theta_{11}(z)^2 - \theta_{10}(y)^2\,\theta_{10}(z)^2 - \theta_{01}(y)^2\,\theta_{01}(z)^2.\end{aligned}$$

We conclude by noticing that $\theta_{11}(0) = 0$.

b) The proof is the same. For the first Riemann theta relation one chooses $a = b = 1/2$, $c = d = 0$, $u = v = y + 1/2$, $w = x = z$.
For the second Riemann theta relation one chooses:
$a = 1/2$, $b = -1/2$, $c = d = 0$, $u = y + 1/2$, $v = y - 1/2$, $w = x = z$.

c) Set $y = 0$ in the previous formulas.

d) Set $z = 0$ in the previous formulas. □

Exercise 4.18. Using the addition formula, prove that the theta-constants $\theta_{a,b}$ are related to the theta-constants $\theta_{[0]}$ and $\theta_{[1]}$ by the formulas

$$\begin{array}{rcl}\theta^2_{00}(0,\tau) & = & \theta^2_{[0]}(0,\tau) + \theta^2_{[1]}(0,\tau),\\ \theta^2_{01}(0,\tau) & = & \theta^2_{[0]}(0,\tau) - \theta^2_{[1]}(0,\tau),\\ \theta^2_{10}(0,\tau) & = & 2\,\theta_{[0]}(0,\tau)\,\theta_{[1]}(0,\tau).\end{array}$$

Exercise 4.19. Prove that for z in $\mathbb{C}$, $\tau \in \mathbb{H}$, one has

$$\begin{array}{rcl}\theta_{00}(0)^2\,\theta_{01}(z)^2 & = & \theta_{10}(0)^2\,\theta_{11}(z)^2 + \theta_{01}(0)^2\,\theta_{00}(z)^2\\ \theta_{00}(0)^2\,\theta_{10}(z)^2 & = & \theta_{10}(0)^2\,\theta_{00}(z)^2 - \theta_{01}(0)^2\,\theta_{11}(z)^2.\end{array}$$

Indication: replace z by $z + 1/2$.

4.7 Projective embeddings

The theta functions are useful to construct projective embeddings both of the elliptic curves but also of the modular curves We just give two examples below.

Projective embedding of elliptic curves The theta functions give an embedding of the elliptic curve $E_\tau := \mathbb{C}/(\mathbb{Z}\tau \oplus \mathbb{Z})$ inside $\mathbb{P}^2(\mathbb{C})$ whose image is a cubic curve.

Proposition 4.20. *The holomorphic map $\psi : \mathbb{C} \to \mathbb{P}^2(\mathbb{C})$ given by*

$$z \mapsto [\theta_{11}(z)\theta_{00}(z)^2, \theta_{00}(z)\theta_{01}(z)\theta_{10}(z), \theta_{11}(z)^3]$$

induces an isomorphism Ψ from E_τ to the smooth cubic C with equation

$$Y^2Z = X(aX - bZ)(bX + aZ)$$

where $a = \dfrac{\theta_{10}(0)^2}{\theta_{00}(0)^2}$ and $b = \dfrac{\theta_{01}(0)^2}{\theta_{00}(0)^2}$.

Proof. We denote by ψ_k, the three functions above so that $\psi = [\psi_1, \psi_2, \psi_3]$. These three functions satisfy

$$\psi_k(z+1) = -\psi_k(z) \text{ and } \psi_k(z+\tau) = -e^{-3i\pi\tau}e^{-6i\pi z}\psi_k(z).$$

Moreover, by Lemma 4.1 they have no joint zeros. Hence they define a holomorphic map $\Psi : E_\tau \to \mathbb{P}^2(\mathbb{C})$. By Corollary 4.17.*c*, the image of Ψ is included in the cubic C. By Corollary 4.17.*d*, the three roots 0, b/a and $-a/b$ are distinct. Hence this cubic C is smooth. Both E and C are smooth compact complex curves. One has $\Psi^{-1}([0,1,0]) = \{0\}$ and near this point $0 \in E$, the map Ψ reads as $z \mapsto [c_1 z + O(z^2), c_2 + O(z), c_3 z^3 + O(z^4)]$ for non zero constants c_i. This proves that the map Ψ has degree 1. Therefore this map Ψ an isomorphism between E_τ and C. □

Projective embedding of the modular curve $X(2)$

The theta functions give also embeddings of modular curves. For $m \geqslant 1$, the modular curve of level m is the quotient $X(m) := \Gamma(m)\backslash\mathbb{H}$. This quotient $X(m)$ is a Riemann surface with finitely many cusps whose genus can be calculated thanks to Hurwitz formula.

In the following lemma we will only deal with $m = 2$. This quotient $X(2)$ is obtained from the fundamental domain for $\Gamma(2)$ on $\mathbb{H}$

$$D := \{\tau \in \mathbb{H} \mid |\mathrm{Re}(\tau)| \leqslant 1, |2\tau - 1| \geqslant 1, |2z + 1| \geqslant 1\}$$

by glueing the two half-lines $\mathrm{Re}(\tau) = \pm 1$ in ∂D thanks to $\tau \to \tau + 2$, and the two half-circles $|2\tau \pm 1| = 1$ thanks to $\tau \to \frac{\tau}{2\tau+1}$. This shows that the surface $X(2)$ has genus zero and three cusps, which means that $X(2)$ is homeomorphic to a 2-sphere minus 3 points. The following lemma gives a nice interpretation of this fact.

Lemma 4.21. *The map* $\varphi : \mathbb{H} \to \mathbb{P}^1(\mathbb{C})$ *given by* $\varphi(\tau) := \dfrac{\theta_{01}(0,\tau)^4}{\theta_{00}(0,\tau)^4}$ *induces a biholomorphism*

$$\Phi : X(2) \ \longrightarrow\ \mathbb{P}^1\mathbb{C} \smallsetminus \{0, \infty, 1\}.$$

Sketch of Proof of Lemma 4.21.

First step: We check that, for all σ in $\Gamma(2)$ and all τ in $\mathbb{H}$ one has $\varphi(\sigma\tau) = \varphi(\tau)$. We only need to check it for the generators $\sigma = u^2$ and $\sigma = v^2$ of $\Gamma(2)$. In these cases, the calculation follows from Exercise 4.15.

Second step: We check that, for all τ in $\mathbb{H}$, one has $\varphi(\tau) \neq 0, \infty, 1$. This follows from Corollary 4.17.*d* and the non vanishing of the theta constants $\theta_{00}(0,\tau)$, $\theta_{01}(0,\tau)$, $\theta_{10}(0,\tau)$ proven in Lemma 4.1.

Third step: We check that the map Φ is proper. Let p_n be sequence in $X(2)$ that goes to one of the three cusps. We want to prove that $\Phi(p_n)$ converges to either $0, 1$, or ∞. Using the equivariance of φ from Exercise 4.23 below, one can assume that p_n converges to the cusp ∞. In that case, our assertion follows from the equality $\lim\limits_{\mathrm{Im}(\tau)\to\infty} \varphi(\tau) = 1$. More precisely, if we set $q = e^{i\pi\tau}$, one has

$$\varphi(\tau) = \tfrac{(\sum_n (-q)^{n^2})^4}{(\sum_n q^{n^2})^4} = 1 - 16q + O(q^2). \tag{4.25}$$

Fourth step: We check that the map Φ is onto. Since the map Φ is open and proper, this follows from Exercise 4.22 below.

Fifth step: We check that, the map Φ is one to one. We know that Φ is a ramified cover. We want to prove that the degree d of this cover is 1.

Either one can compute the degree near the cusp ∞ of $X(2)$, i.e. around $q = 0$, by using Formula (4.25) and gets $d = 1$.

Or one can apply Hurwitz formula to the ramified cover Φ between two surfaces both being a three holed sphere and also gets $d = 1$. □

Exercise 4.22. Prove that a continuous proper open map Φ between two connected locally compact spaces X and Y is onto.

Exercise 4.23. Prove that the map φ is equivariant under $\mathrm{SL}(2, \mathbb{Z})$, and more precisely, that

$$\varphi(-\overline{\tau}) = \overline{\varphi(\tau)}\ \ ,\ \ \varphi(\tau+1) = 1/\varphi(\tau) \text{ and } \ \varphi(-1/\tau) = 1 - \varphi(\tau)\,.$$

Notes to Chapter 4. See [35].

5 Convolution and square

In this lecture we will deal with a finite abelian group G of odd order d, which, most of the time, will be the cyclic group $G = \mathbb{Z}/d\mathbb{Z}$, and with the functional equation

$$f * f\,(2k) = \lambda\, f^2(k) \quad \text{for all } k \text{ in } G, \tag{5.1}$$

where the unknown is a non-zero function $f : G \to \mathbb{C}$ and where $\lambda \in \mathbb{C}$ is a parameter. This equation expresses a proportionality condition between the "convolution square" of f and its "multiplication square".

One of the motivations of Proposition 5.4 and Theorem 5.6 below is to explain some of the intriguing patterns that occur in the lists of possible values of λ obtained by computer experiments.

5.1 Definition and Examples

A non-zero solution f of this functional equation (5.1) will be called a "λ-critical function on G" or, in short, a "λ-critical function", and a value λ for which such a function f exists will be called a "critical value on G", or a "d-critical value" when $G = \mathbb{Z}/d\mathbb{Z}$. Note that Equation (5.1) has been chosen so that it is invariant by translation on the variable k. This equation (5.1) can be rewritten as

$$\sum_{\ell \in G} f(k+\ell)\, f(k-\ell) = \lambda\, f(k)^2 \quad \text{for all } k \text{ in } G. \tag{5.2}$$

Examples Here is the complete list of d-critical values for $d \leqslant 11$ obtained by solving the algebraic equations (5.2) thanks to computer program. Up to sign we will explain in this lecture why all these values are d-critical. The sign issue is more subtle and will be only partially discussed here.

⋆ When $d = 3$, the list of critical values is: $\lambda = 1$, 3, and $\pm i\sqrt{3}$.
⋆ When $d = 5$, the list of critical values is: $\lambda = 1$, 5, $\pm\sqrt{5}$, and $1 \pm 2i$.
⋆ When $d = 7$, the list of critical values is: $\lambda = 1$, 7, $\pm i\sqrt{7}$, and $\pm 2 \pm i\sqrt{3}$.
⋆ When $d = 9$, $\lambda = 1$, 9, $\pm i\sqrt{3}$, $\pm 3i\sqrt{3}$, 3, $\pm\sqrt{5} \pm 2i$, $\pm 1 \pm 2i\sqrt{2}$.
⋆ When $d = 11$, $\lambda = 1$, 11, $4 \pm \sqrt{5}$, $\pm i\sqrt{11}$, $2 \pm i\sqrt{7}$, $\pm 2\sqrt{2} \pm i\sqrt{3}$,
and $\lambda = \pm(1+\varepsilon\sqrt{5}) \pm i\sqrt{5-2\varepsilon\sqrt{5}}$ with $\varepsilon = \pm 1$.

$\star$ The values $\lambda = 1$, resp. $\lambda = d$ are d-critical with $f = \delta_0$, resp. $f = \mathbf{1}_G$.

$\star$ The values $\lambda = \sqrt{d}$ when $d \equiv 1 \bmod 4$ and $\lambda = i\sqrt{d}$ when $d \equiv 3 \bmod 4$ are d-critical values with critical function $f(k) := \eta_d^{k^2}$ where $\eta_d := -e^{i\pi/d}$. Indeed, one has $f * f(2k) = \sum\limits_{1 \leqslant \ell \leqslant d} \eta^{(k-\ell)^2}\eta^{(k+\ell)^2} = \sum\limits_{1 \leqslant \ell \leqslant d} \eta^{2\ell^2}\eta^{2k^2} = \lambda f(k)^2$, where we used the value of the Gauss sum in Lemma 1.5.

$\star$ The value $\lambda = \chi(4)J(\chi, \chi)$, where χ is a Dirichlet character on $\mathbb{Z}/d\mathbb{Z}$ whose square χ^2 is primitive, is a d-critical value with λ-critical function $f = \chi$. Indeed, since both χ and χ^2 are primitive, using Proposition 1.18.*c*, one computes $\chi * \chi(2k) = J(\chi, \chi)\chi^2(2k) = \chi(4)J(\chi, \chi)\chi^2(k)$.

For instance, when $d = 11$, the critical values $\lambda = \pm(1+\varepsilon\sqrt{5}) \pm i\sqrt{5 - 2\varepsilon\sqrt{5}}$ with $\varepsilon = \pm 1$, are obtained this way, choosing for χ either a character of order 5 or a character of order 10.

$\star$ When d' divides d, every d'-critical value is also a d-critical value.

$\star$ When $d = d'd''$ with d' and d'' coprime the product $\lambda = \lambda'\lambda''$ of a d'-critical value and a d''-critical value is a d-critical value. Just because the group $\mathbb{Z}/d\mathbb{Z}$ is isomorphic to the product $\mathbb{Z}/d'\mathbb{Z} \times \mathbb{Z}/d''\mathbb{Z}$.

$\star$ The values $\lambda = \frac{d-3 \pm \sqrt{(d-1)(d-9)}}{2}$ are d-critical values. This follows from the following exercise.

Exercise 5.1. Let $G = \mathbb{Z}/d\mathbb{Z}$ and $f = \alpha\delta_0 + \mathbf{1}_{G \smallsetminus \{0\}}$ with $\alpha \neq 1$.
a) Prove that $\mathbf{1}_{G \smallsetminus \{0\}} * \mathbf{1}_{G \smallsetminus \{0\}} = (d-1)\delta_0 + (d-2)\mathbf{1}_{G \smallsetminus \{0\}}$.
b) Prove that $f * f = (\alpha^2 + d - 1)\delta_0 + (2\alpha + d - 2)\mathbf{1}_{G \smallsetminus \{0\}}$.
c) Prove that $f^2 = \alpha^2\delta_0 + \mathbf{1}_{G \smallsetminus \{0\}}$.
d) Prove that f is λ-critical if and only if $\lambda = 2\alpha + d - 2$ where α is a root of $2\alpha^2 + (d-1)\alpha + d - 1 = 0$.

Exercise 5.2. **Jacobi sums** Let $\zeta_6 = e^{i\pi/3}$.
a) Prove that there exists a Dirichlet character χ of $\mathbb{Z}/7\mathbb{Z}$ such that $\chi(3) = \zeta_6$.
b) Prove that the Jacobi sum $J(\chi, \chi)$ is equal to $2 - \zeta_6^2$.
c) Deduce that $\lambda = -2 + i\sqrt{3}$ is a 7-critical value.

Exercise 5.3. **Critical functions of quadratic residues.** Let $p \geqslant 3$ be prime with $p \equiv 3 \bmod 8$. Let χ_0 be the Legendre character. Remember that $\chi_0(-1) = \chi_0(2) = -1$. Let α, β in $\mathbb{C}^*$ and $f = \alpha\delta_0 + \mathbf{1}_{\mathbb{F}_p^*} + \beta\chi_0$.
a) Prove that $\mathbf{1}_{\mathbb{F}_p^*} * \chi_0 = -\chi_0$.
b) Prove that $\chi_0 * \chi_0 = (1-p)\delta_0 + \mathbf{1}_{\mathbb{F}_p^*}$.

c) Prove that $f^2 = \alpha^2\delta_0 + (1+\beta^2)\mathbf{1}_{\mathbb{F}_p^*} + 2\beta\chi_0$.
d) Prove that $f*f = (\alpha^2+(p-1)(1-\beta^2))\delta_0+(2\alpha+p-2+\beta^2)\mathbf{1}_{\mathbb{F}_p^*}+2(\alpha-1)\beta\,\chi_0$.
e) Prove that f is λ critical if and only if

$$\alpha = 1-\lambda, \quad (\lambda-1)^3 = (p-1)(1-\beta^2) \text{ and } (\lambda-1)\beta^2 = p-3\lambda.$$

f) Prove that the roots of $\lambda^4 - 4\lambda^3 + 6\lambda^2 - 4p\lambda + p^2 = 0$ are p-critical.
g) Let $n = (p-1)/2$. Deduce that $1+\sqrt{n}+i\sqrt{n-2\sqrt{n}}$ is a p-critical value.

5.2 Properties of critical values

We first begin by a few properties of the critical values, that are valid on any finite abelian group.

Proposition 5.4. *Let G be a finite abelian group of odd order d, and λ a critical value on G, then:*
a) *one has $|\lambda| \leqslant d$ with equality if and only if $\lambda = d$,*
b) *there exist only finitely many critical values on G,*
c) *the value λ is algebraic and its Galois conjugates are critical values on G,*
d) *the ratio d/λ is a critical value on G,*
e) *The ratio $\frac{\lambda-1}{2}$ is an algebraic integer.*

Proof of Proposition 5.4. *a*) This follows from Cauchy-Schwarz inequality. Indeed, setting
$\|f\|_\infty = \max_{k\in G} |f(k)|$ and $\|f\|_2 = (\sum_k |f(k)|^2)^{\frac{1}{2}}$, one has

$$|\lambda| \|f\|_\infty^2 = \|f \star f\|_\infty \leqslant \|f\|_2^2 \leqslant d\,\|f\|_\infty^2.$$

Hence $|\lambda| \leqslant d$. In case we have equality the function f must have constant modulus, and must satisfy $f(k+\ell)f(k-\ell) = f(k)^2$, for all k, ℓ. Hence f is proportional to a character and one has $\lambda = d$.

b) The set $X = \{(\lambda, f) \in \mathbb{C}\times\mathbb{C}^G \mid f*f(2k) = \lambda f^2(k) \text{ and } f(0) = 1\}$ is an algebraic variety and the set C of critical values on G is the image of X by the map $(\lambda, f) \mapsto \lambda$.

Therefore, by the elimination of quantifiers in an algebraically closed field, i.e. by Chevalley theorem in Fact 2.11, the set of critical values for G is either finite or has finite complement in $\mathbb{C}$. Since, by Point *a*), this set C is bounded it must be finite.

c) Equations (5.2) have rational coefficients. Hence the images of λ by automorphisms of the field $\mathbb{C}$ are also critical values. Hence, by Point *b*), λ has only finitely many Galois conjugates and λ is algebraic.

d) If f is a λ-critical function on G, then its Fourier transform $\widehat{f}$, which is given by, for every character $\omega : G \to \mathbb{C}^*$,

$$\widehat{f}(\omega) = \tfrac{1}{\sqrt{d}} \sum_{k \in G} f(k)\omega(k),$$

is a d/λ-critical function on the dual group $\widehat{G}$. Since this dual group $\widehat{G}$ is isomorphic to G, d/λ is also a critical value on G.

e) Let G_+ be a subset of G of cardinality $\frac{d-1}{2}$ such that for each non-zero $\ell \in G$ either ℓ or $-\ell$ is in G_+. The equations (5.2) can be rewritten as

$$\tfrac{\lambda-1}{2}\, f(k)^2 = \sum_{\ell \in G_+} f(k+\ell)\, f(k-\ell) \qquad \text{for all } k \text{ in } G \tag{5.3}$$

We will now use Fact 5.5, which says that, to prove that $\lambda' := \frac{\lambda-1}{2}$ is an algebraic integer, it is enough to check that, for all non-archimedean absolute value $|.|_v$ on $\mathbb{C}$, one has $|\lambda'|_v \leqslant 1$.

We set $\|f\|_v := \max\limits_{\ell \in G} |f(\ell)|_v$, we choose k such that $\|f\|_v = |f(k)|_v$, and we compute

$$\begin{aligned} |\lambda'|_v \|f\|_v^2 = |\lambda' f(k)^2|_v \;&=\; |\sum_{\ell \in G_+} f(k+\ell) f(k-\ell)|_v \\ &\leqslant\; \max_{\ell \in G} |f(k+\ell)|_v |f(k-\ell)|_v \;\leqslant\; \|f\|_v^2. \end{aligned}$$

This proves that $|\lambda'|_v \leqslant 1$ as required. □

We have used the following fact:

Fact 5.5. *A complex number $x \in \mathbb{C}$ is an algebraic integer, if and only if, for all ultrametric absolute value $|.|_v$ on $\mathbb{C}$, one has $|x|_v \leqslant 1$.*

Sketch of proof. We first note that when L/K is a field extension, any absolute value on K can be extended to an absolute value on L, see [33, XII,§4]. Hence it is enough to construct the absolute value on the field $\mathbb{Q}(x)$.

When x is transcendental, for all prime $p \geqslant 2$, there is an embedding $i : \mathbb{Q}(x) \hookrightarrow \mathbb{Q}_p$ with $|i(x)|_p > 1$.

When x is algebraic the fractional ideal (x) in K has a decomposition as a finite product of powers $(x) = \prod \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ of prime ideal of the ring of integers $\mathcal{O}_K$. The element x is not in $\mathcal{O}_K$ if and only if one of the valuations $v_{\mathfrak{p}}(x)$ is negative. The corresponding absolute value satisfies $|x|_{\mathfrak{p}} > 1$. □

5.3 Construction of critical values

From now on, G will be the cyclic group $\mathbb{Z}/d\mathbb{Z}$.

Theorem 5.6. *Let a,b be positive integers with $a{+}b{=}d$ and $a \equiv \frac{(d+1)^2}{4} \bmod 4$. Then the complex number $\lambda := \sqrt{a} + i\sqrt{b}$ is a d-critical value.*

Remark 5.7. The congruence assumption in Theorem 5.6 is equivalent to

$$a - b \equiv 1 \bmod 4 \quad \text{and} \quad ab \equiv 0 \bmod 4. \tag{5.4}$$

A more concrete way to state Theorem 5.6 is:

For $d \equiv 1 \bmod 4$, the following values are d-critical:
$\sqrt{d}$, $\sqrt{d{-}4}{+}i\sqrt{4}$, $\sqrt{d{-}8}{+}i\sqrt{8}$, $\sqrt{d{-}12}{+}i\sqrt{12}$, ...

For $d \equiv 3 \bmod 4$, the following values are d-critical:
$i\sqrt{d}$, $\sqrt{4}{+}i\sqrt{d{-}4}$, $\sqrt{8}{+}i\sqrt{d{-}8}$, $\sqrt{12} + i\sqrt{d{-}12}$, ...

More precisely, we will see that, surprisingly, for these values λ, the set of λ-critical functions f with $f(0) = 1$ has positive dimension. Indeed, we will construct a one-parameter family of λ-critical functions using a suitable Jacobi theta function.

We first explain that the congruence condition on the integer a is necessary.

Lemma 5.8. *Let a,b be positive integers and let $\lambda := \sqrt{a}{+}i\sqrt{b}$. The number $\frac{\lambda-1}{2}$ is an algebraic integer if and only if $a{-}b{-}1{\equiv}ab{\equiv}0 \bmod 4$.*

As seen in (5.4), this condition is equivalent to $a \equiv \frac{(d+1)^2}{4} \bmod 4$ where $d := a{+}b$.

In particular, by Proposition 5.4, when this condition is not satisfied, the complex number $\lambda = \sqrt{a} + i\sqrt{b}$ can not be a d-critical value.

Exercise 5.9. For any algebraic number λ, one has the equivalence:
$\nu {:=} \frac{\lambda-1}{2}$ is an algebraic integer $\iff$ $\nu' {:=} \frac{\lambda^2-1}{4}$ is an algebraic integer.
Indic. These two elements ν and ν' are related by the equation $\nu^2 + \nu = \nu'$.

Exercise 5.10. Let $u, v \in \mathbb{Q}$ be two rational numbers. Assume that both v and uv are not squares. Denote by $\sqrt{u}$ and $\sqrt{v}$, one of the two square roots of u and v, respectively. Then, one has the equivalence:

$\mu := \sqrt{u} + \sqrt{v}$ is an algebraic integer $\iff$ $4u \in \mathbb{Z}$ and $v - u \in \mathbb{Z}$.
Indication: Let σ be the Galois automorphism of $\mathbb{Q}[\sqrt{u}, \sqrt{v}]/\mathbb{Q}[\sqrt{u}]$ such that $\sigma(\sqrt{v}) = -\sqrt{v}$. Note that μ is an algebraic integer if and only if both $\mu + \sigma(\mu)$ and $\mu\,\sigma(\mu)$ are algebraic integers.

Proof of Lemma 5.8. The number $\nu' := \frac{\lambda^2-1}{4}$ is equal to $\nu' = \frac{a-b-1}{4} + i\frac{\sqrt{ab}}{2}$. It is an algebraic integer if and only if both $T := \frac{a-b-1}{2}$ and $N := \frac{T^2+ab}{4}$ are integers. This happens if and only if $a-b \equiv 1 \bmod 4$ and $ab \equiv 0 \bmod 4$. □

Corollary 5.11. *Let p,q be positive integers with p odd and q even and let $d := p^2 + q^2$. Then the complex number $\lambda := p + iq$ is a d-critical value.*

Proof. Condition (5.4) is true: $p^2 - q^2 \equiv 1 \bmod 4$ and $p^2 q^2 \equiv 0 \bmod 4$. □

Remark 5.12. It is not known under which condition on these integers p and q, the opposite value $\lambda := -p - iq$ is also d-critical. Even when $q = 0$.

5.4 Using theta functions

Theorem 5.6 is a special case of the following Proposition that gives an explicit family of λ-critical functions thanks to the theta functions (4.1) that we studied in the previous lecture.

Proposition 5.13. *Let a,b be positive integers with $a \equiv \frac{(d+1)^2}{4} \bmod 4$ and $a+b=d$. Set $\lambda_0 := \sqrt{a} + i\sqrt{b}$ and*

$$\tau_0 \ := \ \tfrac{1}{4d^2}(a - b - d^2 + 2i\sqrt{ab}). \tag{5.5}$$

Then for all z in $\mathbb{C}$ the function $k \mapsto \theta_{\tau_0}(z + k/d)$ is λ_0-critical on $\mathbb{Z}/d\mathbb{Z}$.

This means that, for all z in $\mathbb{C}$,

$$\sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} \theta(z + \ell/d, \tau_0)\, \theta(z - \ell/d, \tau_0) \ = \ \lambda\, \theta(z, \tau_0)^2.$$

One can check that these values τ_0 are the simplest one for which Proposition 5.13 holds true.
⋆ For $d = 5$ and $\lambda_0 = 1 + 2i$, one has $\tau_0 = \frac{-7+i}{25}$.
⋆ For $d = 7$ and $\lambda_0 = 2 + i\sqrt{3}$, one has $\tau_0 = \frac{-12+i\sqrt{3}}{49}$.
Without the general formula (5.5), these values of τ_0 are not easy to guess.

5.5 The condition on theta contants

The first step in the proof of Proposition 5.13 is the following criterion on λ, τ which ensures that these functions are λ-critical. This criterion is a relation between "theta constants", i.e. theta functions evaluated at $z = 0$.

Lemma 5.14. *Let $\tau \in \mathbb{H}$ and $\lambda \in \mathbb{C}$. The function $k \mapsto \theta_\tau(z + k/d)$ is λ-critical on $\mathbb{Z}/d\mathbb{Z}$, for all $z \in \mathbb{C}$ if and only if one has the equalities*

$$\lambda = d\,\frac{\theta_{[0]}(0, d^2\tau)}{\theta_{[0]}(0, \tau)} = d\,\frac{\theta_{[1]}(0, d^2\tau)}{\theta_{[1]}(0, \tau)}\ . \tag{5.6}$$

Proof. For w in $\mathbb{C}$ we introduce the function

$$z \mapsto F_w(z) = F_w(z, \tau) := \theta(z + w, \tau)\,\theta(z - w, \tau).$$

We want to know when the two functions $\sum_\ell F_{\ell/d}$ and $F_0 = \theta^2$ are proportional. The key point of the proof is that all these functions F_w live in the same two-dimensional vector space and that this vector space has a very convenient basis: $(\theta_{[0]}, \theta_{[1]})$ that we introduced in (4.6) and (4.7). We only have to express that the coefficients of our two functions in this basis are proportional. These coefficients are given by the following calculation in which we apply successively the addition formula (4.10) and the isogeny formula in Corollary 4.8,

$$\begin{aligned}
\sum_{1\leqslant\ell\leqslant d} F_{\ell/d}(z, \tau) &= \sum_{1\leqslant\ell\leqslant d} \theta_{[0]}(\ell/d, \tau)\,\theta_{[0]}(z, \tau) + \sum_{1\leqslant\ell\leqslant d} \theta_{[1]}(\ell/d, \tau)\,\theta_{[1]}(z, \tau) \\
&= d\,\theta_{[0]}(0, d^2\tau)\,\theta_{[0]}(z, \tau) + d\,\theta_{[1]}(0, d^2\tau)\,\theta_{[1]}(z, \tau) \quad \text{and}
\end{aligned}$$

$$\theta(z, \tau)^2 = \theta_{[0]}(0, \tau)\,\theta_{[0]}(z, \tau) + \theta_{[1]}(0, \tau)\,\theta_{[1]}(z, \tau).$$

These two functions are proportional with proportionality factor λ if and only if one has

$$\lambda = d\,\frac{\theta_{[0]}(0, d^2\tau)}{\theta_{[0]}(0, \tau)} = d\,\frac{\theta_{[1]}(0, d^2\tau)}{\theta_{[1]}(0, \tau)}\ .$$

This is the criterion (5.6). □

The following corollary of Lemma 4.9 looks now very useful. Note that this corollary requires σ to belong to a smaller congruence subgroup $\Gamma(m)$ as defined in (4.11).

Corollary 5.15. *If* $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma(4)$, $\gamma > 0$, *then, for all* τ *in* $\mathbb{H}$, *one has*

$$\frac{\theta_{[0]}(0,\sigma\tau)}{\theta_{[0]}(0,\tau)} \;=\; \frac{\theta_{[1]}(0,\sigma\tau)}{\theta_{[1]}(0,\tau)} \;=\; i^{\frac{\delta-1}{2}} \left(\tfrac{2\gamma}{\delta}\right) (\gamma\tau+\delta)^{\frac{1}{2}} \ . \tag{5.7}$$

Proof. Let

$$\sigma' = \left(\begin{smallmatrix} \alpha & \beta' \\ \gamma' & \delta \end{smallmatrix}\right) \text{ and } \sigma'' = \left(\begin{smallmatrix} \alpha & \beta'' \\ \gamma'' & \delta \end{smallmatrix}\right),$$

with $\beta' = 2\beta$, $\gamma' = \gamma/2$ and $\beta'' = \beta/2$, $\gamma'' = 2\gamma$, so that

$$\sigma'(2\tau) = 2\sigma\tau \ \text{ and } \ \sigma''(\tau/2) = \tfrac{1}{2}\sigma\tau\,.$$

Since the matrix σ is equal to $\pm\mathbf{1}$ mod 4, the two matrices σ' and σ'' are equal to $\mathbf{1}$ mod 2. Therefore we can apply the transformation formula in Lemma 4.9 to both pairs $(\sigma', 2\tau)$ and $(\sigma'', \tau/2)$. Using the multiplicativity properties of the Jacobi symbol, we see that the following two ratios are given by the same formula

$$\frac{\theta(0,2\sigma\tau)}{\theta(0,2\tau)} = \frac{\theta(0,\frac{1}{2}\sigma\tau)}{\theta(0,\frac{1}{2}\tau)} \;=\; i^{\frac{\delta-1}{2}} \left(\tfrac{2\gamma}{\delta}\right) (\gamma\tau+\delta)^{\frac{1}{2}} \ .$$

We now conclude thanks to Equalities (4.8). □

5.6 Elliptic curves with complex multiplication

We can now end the proof of Proposition 5.13, by explaining why the pair (λ_0, τ_0) satisfies Condition (5.6). The key idea is to find

$$\sigma_0 \in \Gamma(4) \ \text{ such that } \ \sigma_0\tau_0 = d^2\tau_0. \tag{5.8}$$

It is most useful before beginning the calculation to understand geometrically the meaning of this condition (5.8).

We introduce the lattice $\Lambda_{\tau_0} = \mathbb{Z}\tau_0 \oplus \mathbb{Z}1$ of $\mathbb{C}$ so that the compact quotient $E_{\tau_0} := \mathbb{C}/\Lambda_{\tau_0}$ is the elliptic curve associated to τ_0. We will see that the values of $\lambda = \lambda_0$ and $\tau = \tau_0$ in Theorem 5.6 have been chosen so that

the elliptic curve E_{τ_0} has complex multiplication by $\mu_0 := \overline{\lambda_0}^{2}$.

More precisely, they have been chosen so that $\mu_0 \Lambda_{\tau_0} = \Lambda_{d^2\tau_0}$. This means that

$$\begin{aligned} d^2\tau_0 &= \mu_0\,(\alpha\tau_0+\beta), \\ 1 &= \mu_0\,(\gamma\tau_0+\delta), \end{aligned}$$

for a matrix $\sigma_0 = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. We will be cautious and choose $\sigma_0 = \mathbf{1}$ mod 4 so that we can apply Corollary 5.15. In fact we will see that it is possible to choose the entries γ and δ to be equal to $\gamma = 4$ and $\delta = 1$.

Exercise 5.16. Check that the only $\tau_0 \in \mathbb{H}$ satisfying $\sigma_0\tau_0 = d^2\tau_0$ for some $\sigma_0 = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma(4)$ with $\gamma = 4$ and $\delta = 1$, are the one given by (5.5).

We now recall the notation of Proposition 5.13. Let a, b be positive integers with $a \equiv \frac{(d+1)^2}{4}$ mod 4 and $a+b=d$. We introduced the parameter $\tau_0 := \frac{(\sqrt{a}+i\sqrt{b})^2}{4d^2} - \frac{1}{4} \in \mathbb{H}$. We introduce the integer $n_0 := \frac{4a-(d+1)^2}{16}$. In the next lemma we give the precise formula for the matrix σ_0

Lemma 5.17. *Let $\sigma_0 \in \Gamma(4)$ be the matrix*

$$\sigma_0 := \left(\begin{smallmatrix} 1+16n_0 & 4n_0 \\ 4 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 4n_0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 4 & 1 \end{smallmatrix}\right)$$

Then one has $\sigma_0\tau_0 = d^2\tau_0$.

Proof. We first compute $\rho_0 := \frac{\tau_0}{4\tau_0+1}$. We set

$$\mu_0 := (4\tau_0+1)^{-1} = \frac{d^2}{(\sqrt{a}+i\sqrt{b})^2} = (\sqrt{a}-i\sqrt{b})^2 = \overline{\lambda}_0^2.$$

Since $4\tau_0 = \mu_0^{-1} - 1$, we compute

$$\rho_0 = \tfrac{1}{4}(1-\mu_0).$$

Since $d = a+b$, this equation can be rewritten as

$$\begin{aligned} \rho_0 &= \tfrac{1}{4}(1-(\sqrt{a}-i\sqrt{b})^2) \\ &= \tfrac{1}{4}(1-2a+d+2i\sqrt{ab}) \\ &= d^2\tau_0 - \tfrac{1}{4}(4a-d^2-2d-1) \\ &= d^2\tau_0 - 4n_0. \end{aligned}$$

This proves that $\sigma_0\tau_0 = d^2\tau_0$.

We can now end the proof of Proposition 5.13. Applying Lemma 5.14 and Corollary 5.15, together with Lemma 5.17, we deduce that, for all z in $\mathbb{C}$, the functions $k \mapsto \theta_{\tau_0}(z + k/d)$ are λ-critical on $\mathbb{Z}/d\mathbb{Z}$ with

$$\lambda = di^{\frac{\delta-1}{2}} \left(\tfrac{2\gamma}{\delta}\right) (\gamma\tau_0 + \delta)^{\frac{1}{2}}, \tag{5.9}$$

where the square root is the one with positive real part. Since $\gamma = 4$ and $\delta = 1$, this gives $\lambda = (d^2\mu_0^{-1})^{\frac{1}{2}} = \overline{\mu_0}^{\frac{1}{2}} = \sqrt{a} + i\sqrt{b}$, as required. □

Notes to Chapter 5. We followed [9].

6 Abelian varieties

All the critical values λ we have found in the previous lecture belong to a cyclotomic field: there exists $n \geqslant 1$ such that λ is in $\mathbb{Q}[e^{2i\pi/n}]$. We show in the next lecture how to construct new critical values that do not belong to cyclotomic field.

In the previous lecture the proof relied on the restriction of a Jacobi theta function to a torsion subgroup of an elliptic curve with complex multiplication.

The new ingredients in this lecture and the next one will be their higher dimensional analogs: the restriction of a Riemann theta function to a torsion subgroup of an abelian variety with a non trivial ring of endomorphisms.

For instance with this method one can prove that

$$\lambda = 1 + \sqrt{5} + i\sqrt{9 - 2\sqrt{5}} \text{ is 15-critical,} \tag{6.1}$$

$$\lambda = 1 + 2\sqrt{2} + 2i\sqrt{3 - \sqrt{2}} \text{ is 21-critical.} \tag{6.2}$$

In this lecture we focus on the various equivalent definitions of abelian varieties. This topic would deserve a whole book as [14] and the reader is encouraged to go to this book if he wants to know more on the abelian varieties and their theta functions. The aim of this lecture is to state with no proof how unitary $\mathbb{Q}$-endomorphisms of abelian varieties allow us to construct new critical values. The proof will be given in the next lecture thanks to the Riemann theta functions and their addition, isogeny and transformation formulas.

6.1 Kähler bilinear forms and Riemann matrices

We begin this lecture by a few elementary lemmas from linear algebra, that focus on the imaginary part of a hermitian scalar product seen as a symplectic bilinear form. The notion of Riemann matrix will show up as an output of this discussion.

In this lecture dealing with an abelian variety A , we follow the tradition to denote by g its dimension, keeping in mind the important case where where A is the Jacobian of a genus g curve.

Let $V = \mathbb{C}^g$ be a g-dimensional complex vector space and let ω be a real symplectic bilinear form on V. This means that ω is antisymmetric and non-degenerate. For instance the imaginary part $\omega = \mathrm{Im}(H)$ of a positive hermitian form H on $\mathbb{C}^g$.

By convention our hermitian form will be linear in the first variable and antilinear in the second variable: $H(\lambda v, \mu w) = \lambda\overline{\mu}\, H(v,w)$, for all λ in $\mathbb{C}$ and v, w in V, and also $H(w,v) = \overline{H(v,w)}$.

Definition 6.1. *We say that ω is Kähler if there exists a positive hermitian form H on V such that $\omega = Im(H)$.*

Lemma 6.2. *A real symplectic bilinear form ω on V is Kähler if and only if, for all v_1, v_2 in V and $v \neq 0$, one has $\omega(iv_1, iv_2) = \omega(v_1, v_2)$ and $\omega(iv, v) > 0$.*

Proof. One recover the hermitian form thanks to the formula, for v_1, $v_2 \in V$: $H(v_1, v_2) = \omega(iv_1, v_2) + i\omega(v_1, v_2)$. □

For any symplectic bilinear form ω on V there exists a basis of the real vector space V of the form $(f_1, \ldots, f_g, e_1, \ldots, e_g)$ such that

$$\omega(e_j, e_k) = \omega(f_j, f_k) = 0 \ \text{ and } \ \omega(f_j, e_k) = \delta_{j,k} \quad \text{for all } j, k,$$

or equivalently, $\omega = \sum_j f_j^* \wedge e_j^*$.

Remark 6.3. If ω is Kähler, the family $(e_1, \ldots, e_g)$ is a basis of $\mathbb{C}^g$.

Proof. Let V_0 be the real vector space spanned by $e_1, \ldots, e_g$. We want to prove that $V_0 \cap iV_0 = \{0\}$. But when v is in this intersection $V_0 \cap iV_0$, one has $H(v,v) = \omega(iv, v) = 0$ and hence $v = 0$. □

For the same reason $(f_1, \ldots, f_g)$ is a basis of $\mathbb{C}^g$ and we denote by τ the matrix giving the base change. This $g \times g$ complex matrix τ is given by

$$(f_1, \ldots, f_g) = (e_1, \ldots, e_g)\,\tau.$$

This means that the entries of the k^{th} column of the matrix τ are the coordinates of the vector f_k in the basis e_j, that is $f_k = \sum\limits_{1 \leqslant j \leqslant g} \tau_{jk} e_j$ for all $k \leqslant g$.

Definition 6.4. *A $g \times g$ complex matrix τ is called a Riemann matrix if τ is symmetric and its imaginary part is positive definite.*

Lemma 6.5. *The real symplectic bilinear form ω on V is Kähler if and only if τ is a Riemann matrix.*

Proof. We write $\tau = R + iS$ where R and S are $g \times g$ real matrices. We want to prove that both R and S are symmetric and that S is positive definite.

We write the base change between the following two real basis of V

$$(f_1, \dots, f_g, e_1, \dots, e_g) \;=\; (e_1, \dots, e_g, ie_1, \dots, ie_g) \begin{pmatrix} R & \mathbf{1} \\ S & 0 \end{pmatrix} \tag{6.3}$$

Therefore the antisymmetric matrix Ω that expresses ω in this second real basis $(e_1, \dots, e_g, ie_1, \dots, ie_g)$ is

$$\begin{aligned} \Omega &= {}^t\begin{pmatrix} R & \mathbf{1} \\ S & 0 \end{pmatrix}^{-1} \begin{pmatrix} 0 & \mathbf{1} \\ -\mathbf{1} & 0 \end{pmatrix} \begin{pmatrix} R & \mathbf{1} \\ S & 0 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 0 & \mathbf{1} \\ {}^tS^{-1} & -{}^tS^{-1}{}^tR \end{pmatrix} \begin{pmatrix} 0 & \mathbf{1} \\ -\mathbf{1} & 0 \end{pmatrix} \begin{pmatrix} 0 & S^{-1} \\ \mathbf{1} & -RS^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & -S^{-1} \\ {}^tS^{-1} & {}^tS^{-1}({}^tR - R)S^{-1} \end{pmatrix}. \end{aligned}$$

Therefore, by Lemma 6.2, the symplectic form ω is Kähler if and only if ${}^tR = R$, ${}^tS = S$, and S is positive definite. □

6.2 The Siegel space and the symplectic group

We now introduce the Siegel upper half-space $\mathcal{H}_g$ that will replace the Poincaré upper half-plane. We will also introduce its group of isometries $\mathrm{Sp}(g, \mathbb{R})$ that will replace the group $\mathrm{SL}(2, \mathbb{R})$ (see also [18] or [8]).

It will be convenient to use notation that looks as much as possible like the notation for the case when $g = 1$. This is why we will still use lower case greek letters τ, α, $\beta, \dots$ to denote $g \times g$ matrices.

For $g \geqslant 1$, let $\mathcal{H}_g$ be the Siegel upper half-space which is the space of Riemann matrices of size g,

$$\mathcal{H}_g \;=\; \{\tau \in \mathcal{M}(g, \mathbb{C}) \mid {}^t\tau = \tau,\ \ \mathrm{Im}\,\tau > 0\},$$

where ${}^t\tau$ denotes the transpose of the matrix τ. Let $J = \begin{pmatrix} \mathbf{0} & \mathbf{1}_g \\ -\mathbf{1}_g & \mathbf{0} \end{pmatrix}$ and

$$\mathrm{Sp}(g, \mathbb{R}) := \{\sigma \in \mathrm{GL}(2g, \mathbb{R}) \mid {}^t\sigma J \sigma = J\},$$

be the real symplectic group. This group is the stabilizer of the symplectic form $\omega(x, y) = {}^tx\, J\, y$ on $\mathbb{R}^{2g}$, that is,

$$\mathrm{Sp}(g, \mathbb{R}) = \{\sigma \in \mathrm{GL}(2g, \mathbb{R}) \mid \omega(\sigma x, \sigma y) = \omega(x, y) \text{ for all } x,\ y \text{ in } \mathbb{R}^{2g}\},$$

The group $\mathrm{Sp}(g,\mathbb{R})$, seen as a group of 2 by 2 block real matrices of size g is given by

$$\mathrm{Sp}(g,\mathbb{R}) = \{\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \mid \sigma^{-1} = \left(\begin{smallmatrix} {}^t\delta & -{}^t\beta \\ -{}^t\gamma & {}^t\alpha \end{smallmatrix}\right)\}, \quad \text{or, equivalently}$$

$$\mathrm{Sp}(g,\mathbb{R}) = \{\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \mid {}^t\alpha\gamma = {}^t\gamma\alpha,\ \ {}^t\beta\delta = {}^t\delta\beta,\ \ {}^t\alpha\delta - {}^t\gamma\beta = \mathbf{1}_g\}.$$

Lemma 6.6. *The group* $\mathrm{Sp}(g,\mathbb{R})$ *acts transitively on the Siegel upper half-space* $\mathcal{H}_g$ *thanks to the formula*

$$\sigma\tau := (\alpha\tau + \beta)(\gamma\tau + \delta)^{-1}. \tag{6.4}$$

One cannot confuse this notation $\sigma\tau$ with the product of matrices since σ has size $2g$ while τ has size g.

Note that in this formula the involved matrices have no reasons to commute, hence one has to pay attention to the order in which one computes the product of these matrices.

Proof. We first want to check that the matrix $\gamma\tau + \delta$ is invertible. For that one computes using the above relations between the block matrices

$$(\overline{\tau}\ {}^t\alpha + {}^t\beta)(\gamma\tau + \delta) - (\overline{\tau}\ {}^t\gamma + {}^t\delta)(\alpha\tau + \beta) = \overline{\tau} - \tau = 2i\,\mathrm{Im}(\tau). \tag{6.5}$$

Let $v \in \mathbb{C}^g$ be a vector in the kernel of $\gamma\tau+\delta$. By (6.5), one has ${}^t\overline{v}(\overline{\tau}-\tau)v = 0$. Since the matrix $\mathrm{Im}(\tau)$ is positive definite, this implies that $v = 0$. This proves that $\gamma\tau + \delta$ is invertible, and formula (6.4) is well defined. We set $\tau' := \sigma\tau = (\alpha\tau + \beta)(\gamma\tau + \delta)^{-1}$..

We want now to prove that τ' is symmetric. For that we compute

$$(\tau\ {}^t\gamma + {}^t\delta)({}^t\tau' - \tau')(\gamma\tau + \delta) = (\tau\ {}^t\alpha + {}^t\beta)(\gamma\tau + \delta) - (\tau\ {}^t\gamma + {}^t\delta)(\alpha\tau + \beta) = 0.$$

which proves that ${}^t\tau' = \tau'$.

We also check that the imaginary part of τ' is positive definite. This follows from the following calculation based on (6.5),

$$(\overline{\tau}\ {}^t\gamma + {}^t\delta)({}^t\overline{\tau'} - \tau')(\gamma\tau + \delta) = \overline{\tau} - \tau = 2i\,\mathrm{Im}(\tau).$$

Finally we need to check that the action of $\mathrm{Sp}(g,\mathbb{R})$ on $\mathcal{H}_g$ is transitive. Formula (6.3) tells us, that given a symplectic structure on $\mathbb{R}^{2g}$, an element τ of $\mathcal{H}_g$ gives a complex structure on $\mathbb{R}^{2g}$ together with a positive hermitian form H whose imaginary part is ω. Since the group $\mathrm{GL}(2g,\mathbb{R})$ acts transitively on the set of complex structure on $\mathbb{R}^{2g}$ together with a positive hermitian form, the group $\mathrm{Sp}(g,\mathbb{R})$ acts transitively on $\mathcal{H}_g$. □

Exercise 6.7. Prove that the stabilizer in the group $\mathrm{Sp}(g, \mathbb{R})$ of the element $\tau_0 = i\mathbf{1}_g \in \mathcal{H}_g$ is the unitary group $U(g, \mathbb{R})$, so that $\mathcal{H}_g \simeq \mathrm{Sp}(g, \mathbb{R})/\mathrm{U}(g, \mathbb{R})$.

Remark 6.8. This means that $\mathcal{H}_g$ is the Riemannian symmetric space G/K associated to the semisimple Lie group $G = \mathrm{Sp}(g, \mathbb{R})$ and its maximal compact subgroup $K = \mathrm{U}(g, R)$. This symmetric space is a hermitian symmetric space: it admits a G-invariant hermitian structure.

6.3 Integral symplectic bilinear forms

Before introducing abelian varieties, we need to recall the theory of integral symplectic bilinear forms.

Lemma 6.9. *Let $\Lambda = \mathbb{Z}^{2g}$ and ω be an integral symplectic bilinear form on Λ. Then there exists a positive integral diagonal matrix $\Delta = \mathrm{diag}(d_1, \ldots, d_g)$ with $d_1 | d_2 | \cdots | d_g$ and a $\mathbb{Z}$-basis $(f_1, \ldots, f_g, e_1, \ldots, e_g)$ of $\mathbb{Z}^{2g}$ such that the matrix of ω in this basis is $\left(\begin{smallmatrix} 0 & \Delta \\ -\Delta & 0 \end{smallmatrix}\right)$.*

Proof. Let $d > 0$ be the minimum positive value for $\omega(v, w)$ with v, w in Λ. Choose two vectors f and e in Λ such that $\omega(f, e) = d$. Note that, because of the Euclid algorithm, one has

$$\omega(e, \Lambda) = \omega(f, \Lambda) = d\mathbb{Z}.$$

Let $\Lambda' := \{v' \in \Lambda \mid \omega(f, v') = \omega(e, v') = 0\}$ be the orthogonal in Λ of $\mathbb{Z}f \oplus \mathbb{Z}e$ for ω. Since for all v in Λ the element

$$v' := v - \tfrac{\omega(f,v)}{d} e - \tfrac{\omega(v,e)}{d} f$$

belongs to Λ', one has the equality

$$\Lambda = (\mathbb{Z}f \oplus \mathbb{Z}e) \oplus \Lambda'.$$

We can now conclude by induction. It only remains to check that for all v', w' in Λ' the integer $\omega(v', w')$ is a multiple of d. We write $\omega(v', w') = dq + r$ with q, r integers such that $0 \leqslant r < d$, and we want to prove that $r = 0$. We compute

$$\omega(v' - qf, w' + e) = \omega(v', w') - qd = r.$$

Hence by minimality of d, one has $r = 0$ as required. □

6.4 Polarized abelian varieties

We now introduce the principally polarized abelian varieties that will replace the elliptic curves. A new phenomenon occurs in dimension $g \geqslant 2$: not all the complex tori $\mathbb{C}^g/\Lambda$, admits a holomorphic embedding in a complex projective space $\mathbb{P}(\mathbb{C}^N)$.

Definition 6.10. *A polarized abelian variety $(A = V/\Lambda, \omega)$ is a complex torus, where $V = \mathbb{C}^g$ and Λ is a lattice in V, together with a real symplectic bilinear form $\omega : V \times V \to \mathbb{R}$ on V satisfying the following two conditions:*
(i) the symplectic form ω takes integral values on $\Lambda \times \Lambda$, and
(ii) ω is the imaginary part $\mathrm{Im}(H)$ of a positive hermitian form H on V.

Before going on we need to explain why this definition which involves only notion from linear algebra is useful. We first recall that a Kähler manifold is a complex manifold X endowed with a symplectic differential form ω which is equal to the imaginary part $\omega := ImH$ of a hermitian structure on X. This form ω is called a Kähler form. Two Kähler structure are said to be equivalent if the corresponding symplectic forms are cohomologous, i.e. they have same image $[\omega]$ in $H^2(X, \mathbb{R})$. The most important Kähler structures are those for which this cohomology class is integral that is $[\omega] \in H^2(X, \mathbb{Z})$.

In case of tori one has the following fact

Fact 6.11. *Let $V = \mathbb{C}^g$, let Λ be a lattice in V and let T be the quotient torus $T = V/\Lambda$. Then one has the equivalences $(i) \Leftrightarrow (ii) \Leftrightarrow (iii) \Leftrightarrow (iv)$.*
(i) The torus T admits a holomorphic embedding in a projective space $\mathbb{P}(\mathbb{C}^N)$.
(ii) The torus T admits an integral Kähler symplectic differential form ω.
(iii) There exists a symplectic bilinear form ω on V such that (T, ω) is a polarized abelian variety.
(iv) There exists a basis $e_1, \ldots, e_g$ of $\mathbb{C}^g$ and a positive integral diagonal matrix $\Delta = \mathrm{diag}(d_1, \ldots, d_g)$ with $d_1|d_2|\cdots|d_g$ and a Riemann matrix $\tau \in \mathcal{H}_g$ such that $\Lambda = \tau\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$.

Condition (i) means that T has a structure of projective algebraic variety.

Sketch of proof.

$(i) \Rightarrow (ii)$ See [18, VI.6]. The main examples of a Kähler manifold is a smooth projective algebraic variety. This is a smooth compact complex submanifold X of $Z := \mathbb{CP}^N$. The Kähler form ω on X is obtained as the restriction to X of the unique $U(N+1)$-invariant normalized Kähler form ω_{FS} on $Z = \mathbb{CP}^N$ which is called the Fubini-study form. The Fubini-Study form is defined by the equality

$$\pi^*(\omega_{FS}) = \tfrac{i}{2\pi}\partial\overline{\partial}\log\|z\|^2 := \tfrac{i}{2\pi}\sum_{j,k}\partial_{z_j}\partial_{\overline{z_k}}\log(\sum_{\ell} z_\ell\overline{z_\ell})\,\mathrm{d}z_j\mathrm{d}\overline{z_k},$$

where $\pi : \mathbb{C}^N \smallsetminus \{0\} \to \mathbb{P}(\mathbb{C}^N)$ is the natural projection. The class $[\omega] \in H^2(X,\mathbb{R})$ of the Kähler form ω is integral, i.e. belongs to $H^2(X,\mathbb{Z})$ because the class $[\omega_{FS}]$ of the Fubini-Study Kähler form ω_{FS} is already integral. This follows from the following calculation.

Let $F : \mathbb{C} \to \mathbb{P}(\mathbb{C}^N)$ be the map given by $F(z) = [1, z, 0, 0, \ldots]$. This map generates $H_2(X,\mathbb{Z})$ and one has

$$\begin{aligned}\int_{\mathbb{C}} F^*(\omega_{FS}) &= \tfrac{i}{2\pi}\int_{\mathbb{C}}\partial_z\partial_{\overline{z}}\log(1+z\overline{z})\,\mathrm{d}z\mathrm{d}\overline{z}\\ &= \tfrac{1}{\pi}\int_0^{2\pi}\int_0^{\infty}(1+r^2)^{-2}r\mathrm{d}r\mathrm{d}\theta \;=\; 1.\end{aligned}$$

(ii) ⇒ *(iii)* See [18, III.4]. All the translates $t^*\omega$ of the Kähler form ω by elements t of the torus T are also integral Kähler forms and hence their cohomology class is constant $[t^*\omega] = [\omega]$. Their average $\omega_0 = \int_T t^*\omega\,\mathrm{d}t$ is a T-invariant Kähler form which is also cohomologous to ω. Therefore ω_0 is a T-invariant integral Kähler form on T. It can be seen as a symplectic bilinear form on V which takes integral values on $\Lambda \times \Lambda$.

(iii) ⇒ *(iv)* See [18, VI.1]. According to the reduction in Lemma 6.9 applied to the non-degenerate integral symplectic bilinear forms ω on $\Lambda\times\Lambda$, there exists a positive integral matrix $\Delta = \operatorname{diag}(d_1,\ldots,d_g)$ with $d_1|d_2|\cdots|d_g$ a basis of Λ of the form $(f_1,\ldots,f_g,d_1e_1,\ldots,d_ge_g)$ such that

$$\omega(e_j,e_k) = \omega(f_j,f_k) = 0 \text{ and } \omega(f_j,e_k) = \delta_{j,k} \quad \text{for all } j,k.$$

According to Lemma 6.5 the family $(e_1,\ldots,e_g)$ is then a basis of $\mathbb{C}^g$. and the $g\times g$ matrix τ given by $(f_1\ldots,f_g) = (e_1,\ldots,e_g)\tau$ satisfies the “Riemann condition”: it is a symmetric complex matrix with positive definite imaginary part, that is τ belongs to $\mathcal{H}_g$.

(iv) ⇒ *(i)* See [14, §4.5] and [18, VI.3]. We just give a hint. The positivity of the imaginary part of τ allows to construct many theta functions on V and hence to construct a holomorphic line bundle on T with sufficiently many

sections. We obtain this way a holomorphic embedding in the projectivized dual of the space of sections of this bundle. □

Remark 6.12. For the proof of $(iv) \Rightarrow (i)$ we can also use the general fact: a compact Kähler manifold X whose Kähler form ω has an integral cohomology class is a projective algebraic variety.

6.5 Principally polarized abelian varieties

Definition 6.13. *A polarization ω on an abelian variety $A = V/\Lambda$ is principal, if the restriction of ω to $\Lambda \times \Lambda$ has determinant* 1.

Equivalently this means that the diagonal matrix Δ is the identity. At first glance, this assumption looks harmless for us since every polarized abelian variety is isogenous to a principally polarized abelian variety. The problem is that changing Λ by a finite index subgroup might change the finite abelian group G on which one constructs a critical function. It is indeed a delicate issue to choose Λ in such a way that G is cyclic.

Fact 6.14. *The map $(A, \omega) \longrightarrow \tau$ given in Fact 6.11.iv induces a bijection*

$$\left\{\begin{matrix} \textit{principally polarized} \\ \textit{abelian varieties} \end{matrix}\right\} \quad \longleftrightarrow \quad \mathrm{Sp}(g, \mathbb{Z})\backslash\mathcal{H}_g. \tag{6.6}$$

Sketch of proof. For τ in $\mathcal{H}_g$, we introduce the lattice

$$\Lambda_\tau := \tau\mathbb{Z}^g \oplus \mathbb{Z}^g$$

of $\mathbb{C}^g$, the quotient torus $A_\tau := \mathbb{C}^g/\Lambda_\tau$, the hermitian form H_τ on $\mathbb{C}^g$ whose matrix is $(\mathrm{Im}\tau)^{-1}$ in the canonical basis $(e_1, \ldots, e_g)$ and the imaginary part ω_τ of H_τ. The pair (A_τ, ω_τ) is then a principally polarized abelian variety, and the map $\tau \mapsto (A_\tau, \omega_\tau)$ is the inverse map of (6.6). □

6.6 Endomorphisms of abelian varieties

Let $(A = V/\Lambda, \omega)$ be a polarized abelian variety.

We denote by $\mathrm{End}(A)$ the ring of endomorphisms $\mu : A \to A$. These are the holomorphic group morphisms $A \to A$. They are given by a complex matrix $T_\mu \in \mathrm{End}(V)$ that preserve the lattice $T_\mu(\Lambda) \subset \Lambda$. An *isogeny of A* is an endomorphism μ of A which is given by an invertible matrix T_μ, i.e. an endomorphism whose kernel $K_\mu \subset A$ is a finite subgroup.

We denote by $\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ the $\mathbb{Q}$-algebra of $\mathbb{Q}$-endomorphisms ν of A. To each $\mathbb{Q}$-endomorphism $\nu \in \mathrm{End}_{\mathbb{Q}}(A)$ is associated
⋆ a *tangent map* $T_\nu \in \mathrm{End}_{\mathbb{C}}(V) \simeq \mathcal{M}(g, \mathbb{C})$,
⋆ a *holonomy map* $h_\nu \in \mathrm{End}_{\mathbb{Q}}(\Lambda_{\mathbb{Q}}) \simeq \mathcal{M}(2g, \mathbb{Q})$, where $\Lambda_{\mathbb{Q}} := \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$.
The map h_ν is the restriction of T_ν to $\Lambda_{\mathbb{Q}}$.

In other words, an endomorphism (resp. $\mathbb{Q}$-endomorphism) ν of A is nothing but a $\mathbb{C}$-endomorphism of V that preserves Λ (resp. $\Lambda_{\mathbb{Q}}$). This is why one sometimes writes abusively ν instead of T_ν or h_ν. But it is useful to keep the two notations because, in coordinates, T_ν is a $g \times g$ complex matrix while h_ν is a $2g \times 2g$ rational matrix.

Lemma 6.15. *Let (A, ω) be a polarized abelian variety and ν be a $\mathbb{Q}$-endomorphism of A. Then there is a unique $\mathbb{Q}$-ensomorphism ν^* of A defined by one of the two equivalent properties:*
⋆ *T_{ν^*} is the adjoint of T_ν for the hermitian form H on V.*
⋆ *h_{ν^*} is the adjoint of h_ν for the symplectic form ω on $\Lambda_{\mathbb{Q}}$.*
The map $\nu \mapsto \nu^*$ is an antiinvolution of the $\mathbb{Q}$-algebra $\mathrm{End}_{\mathbb{Q}}(A)$ called the Rosati antiinvolution.

Proof. Let $T^* \in \mathrm{End}_{\mathbb{C}}(V)$ be the adjoint of T_ν for the hermitian form H and $h^* \in \mathrm{End}_{\mathbb{Q}}(\Lambda_{\mathbb{Q}})$ be the ajoint of h_ν for the symplectic form ω. By definition T^* and h^* are defined by the equalities

$$\begin{aligned} H(T^*v, w) &= H(v, T_\nu w) \text{ for all } v,\ w \text{ in } V, \\ \omega(h^*v, w) &= \omega(v, h_\nu w) \text{ for all } v,\ w \text{ in } \Lambda_{\mathbb{Q}}. \end{aligned}$$

Since $\omega = \mathrm{Im}(H)$ and since h_ν is the restriction of T_ν to $\Lambda_{\mathbb{Q}}$, the map h^* is the restriction of T^* to $\Lambda_{\mathbb{Q}}$. This means that there exists a $\mathbb{Q}$-endomorphism ν^* of A such that $T_{\nu^*} = T^*$ and $h_{\nu^*} = h^*$.

By construction, one has $(\nu_1\nu_2)^* = \nu_2^*\nu_1^*$, for all ν_1, ν_2 in $\mathrm{End}_{\mathbb{Q}}(A)$. □

Corollary 6.16. *Let (A, ω) be a polarized abelian variety and ν be a $\mathbb{Q}$-endomorphism of A. Then, the tangent map T_ν is a unitary transformation of the hermitian space V if and only if the holonomy map h_ν belongs to $\mathrm{Sp}(\Lambda_{\mathbb{Q}}, \omega)$. One has then $\nu\nu^* = \nu^*\nu = 1$, and ν is called a unitary $\mathbb{Q}$-endomorphism of A*

The $\mathbb{Q}$-algebra $R = \mathrm{End}_{\mathbb{Q}}(A)$ with this antiinvolution is an important invariant of the polarized abelian variety A. We just quote the following fact which gives strong restrictions on the algebra R. For ν in R, the rational trace of ν is defined as the trace of its holonomy $Tr_r(\nu) := Tr(h_\nu) \in \mathbb{Q}$.

Fact 6.17. *The $\mathbb{Q}$-algebra $R = \mathrm{End}_{\mathbb{Q}}(A)$ is a semi-simple algebra over $\mathbb{Q}$ and the Rosatti antiinvolution is positive.*

This means that the hermitian form $(\mu, \nu) \mapsto Tr_r(\mu^*\nu)$ on R is positive.

The finite dimensional $\mathbb{Q}$ algebras with a positive antiinvolution have been classified by Albert in the early nineteenth century. The list is very short (See [14, §5.5]).

6.7 Critical values and abelian varieties

We now introduce the condition that will replace the congruence condition in (5.8) in this higher dimensional abelian varieties. It is called the Igusa condition.

For $\ell \geqslant 2$ even, let $\mathbb{Z}_{(\ell)}$ be the ring of rational numbers with denominator prime to ℓ. We introduce the *rational congruence symplectic group of level ℓ*

$$\mathrm{Sp}^{\ell}_{g,\mathbb{Q}} := \{h \in \mathrm{Sp}(g, \mathbb{Z}_{(\ell)}) \mid \sigma \equiv \mathbf{1}_{2g} \bmod \ell\}, \tag{6.7}$$

and the *rational symplectic theta group of level ℓ*

$$\mathrm{Sp}^{\theta,\ell}_{g,\mathbb{Q}} := \{h = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Sp}^{2\ell}_{g,\mathbb{Q}} \mid ({}^t\alpha\gamma)_0 \equiv ({}^t\beta\delta)_0 \equiv 0 \bmod 2\ell\}, \tag{6.8}$$

where for a $g \times g$ symmetric matrix S, the notation S_0 means the diagonal of S.

We will mainly be interested with the value $\ell = 2$. We say that $h \in \mathrm{Sp}(g, \mathbb{Q})$ *preserves a theta structure of level* 2 if it belongs to $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$. The group $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$ is a normal subgroup of the group $\mathrm{Sp}(g, \mathbb{Z}_{(2)})$, and one has the inclusions

$$\mathrm{Sp}^{4}_{g,\mathbb{Q}} \subset \mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}} \subset \mathrm{Sp}^{2}_{g,\mathbb{Q}} \subset \mathrm{Sp}(g, \mathbb{Z}_{(2)}).$$

Indeed the reduction modulo 4 of the group $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$ is the group $\widetilde{\mathrm{Sp}}(g, \mathbb{F}_2)$ which is a normal subgroup of the group $\mathrm{Sp}(g, \mathbb{Z}/4\mathbb{Z}) \simeq \mathrm{Sp}(g, \mathbb{Z}_{(2)})/\mathrm{Sp}^{4}_{g,\mathbb{Q}}$.

Definition 6.18. *We say that the unitary $\mathbb{Q}$-endomorphism ν of A preserves a theta structure of level 2 if the holonomy h_ν belongs to the rational symplectic theta subgroup $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$ of level 2 in a symplectic basis of (Λ, ω). This condition does not depend on the choice of the symplectic basis of Λ.*

The following theorem is the higher dimensional analog of Theorem 5.6

Theorem 6.19. *Let* $(A = \mathbb{C}^g/\Lambda, \omega)$ *be a principally polarized abelian variety,* ν *be a unitary* $\mathbb{Q}$*-endomorphism of* A *preserving a theta structure of level* 2*,* T_ν *its tangent map,* $G_\nu := \nu^{-1}\Lambda/(\Lambda \cap \nu^{-1}\Lambda)$ *and* $d_\nu := |G_\nu|$*. Then there exists a critical value*

$$\lambda_\nu = \kappa_\nu \, d_\nu^{1/2} \, \det_{\mathbb{C}}(T_\nu)^{1/2} \tag{6.9}$$

on the group G_ν *with* $\kappa_\nu^8 = 1$*.*

Remark 6.20. Note that the critical value has absolute value $|\lambda_\nu| = d_\nu^{1/2}$. The square κ_ν^2 can be easily calculated since one knows from Proposition 5.4 that $\frac{1}{2}(\lambda_\nu - 1)$ is an algebraic integer.

The abelian group G_ν depends not only on the tangent map $T_\nu \in \mathcal{M}(g, \mathbb{C})$ but also on the lattice Λ. It might be cyclic even when $g > 1$.

Theorem 6.19 will be proven in the next Lecture by using the restriction of a suitable Riemann theta function to the torsion group G_ν.

Notes to Chapter 6. The main results of this chapter are in [10]. We also used [18] and [14]

7 Riemann Theta functions

In this lecture we give the proof of Theorem 6.19, that tells us how to construct critical values λ on a finite abelian group G starting from an abelian variety A endowed with a unitary $\mathbb{Q}$-endomorphism ν.

The key idea is to think of G as a finite subgroup of A and to find the λ-critical function among the Riemann theta functions. This is why most of this lecture deals with the construction of theta functions and their first properties.

We will end this lecture by explaining how this construction give rise to explicit new critical values when one uses abelian varieties associated to CM Number fields.

This lecture and the previous one should be seen as a quick introductory course to the abelian varieties, their $\mathbb{Q}$-endomorphisms, their theta functions and their links with CM number fields.

7.1 Theta functions

We now introduce the Riemann theta functions that will replace the Jacobi theta functions:

$$\theta_\tau(z) = \theta(z,\tau) := \sum_{m\in\mathbb{Z}^g} e^{i\pi\,{}^t m\tau m} e^{2i\pi\,{}^t m z}, \quad \text{for } z \in \mathbb{C}^g \text{ and } \tau \in \mathcal{H}_g.$$

This function is a holomorphic function of z which is $\mathbb{Z}^g$-periodic. One has $\theta_\tau(z+q) = \theta_\tau(z)$ for all q in $\mathbb{Z}^g$.

We will also need to introduce the Riemann theta functions with characteristic (see [14]). We will also need three classical formulas satisfied by these functions, the “addition formula”, the “isogeny formula”, and the “transformation formula”. We will only need special cases of these formulas that we state below.

The *theta functions with characteristic* a, b in $\mathbb{C}^g$, are defined by, for $z \in \mathbb{C}^g$ and $\tau \in \mathcal{H}_g$,

$$\begin{aligned} \theta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau) &:= \sum_{m\in\mathbb{Z}^g} e^{i\pi\,{}^t(m+a)\tau(m+a)} e^{2i\pi\,{}^t(m+a)(z+b)} \\ &= e^{i\pi\,{}^t a\tau a} e^{2i\pi\,{}^t a(z+b)}\, \theta(z+\tau a+b,\tau). \end{aligned}$$

Again these functions depend only on $b+z$, hence it is not restrictive to study them when $z=0$ and to define

$$\theta_\tau\begin{bmatrix} a \\ b \end{bmatrix} \ := \ \theta\begin{bmatrix} a \\ 0 \end{bmatrix}(b,\tau) \ = \ \theta\begin{bmatrix} a \\ b \end{bmatrix}(0,\tau)$$

These functions also satisfy the following periodicity when translating the characteristic by elements m, n in $\mathbb{Z}^g$,

$$\theta\begin{bmatrix} a+m \\ b+n \end{bmatrix}(z,\tau) \quad = \quad e^{2i\pi {}^t a n}\, \theta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau).$$

The following special cases of theta functions with characteristics will be very useful. For $\xi \in \mathbb{Z}^g/2\mathbb{Z}^g$, seen as a subset of $\mathbb{Z}^g$, we define

$$\theta_{[\xi]}(z,\tau) = \theta\begin{bmatrix} \xi/2 \\ 0 \end{bmatrix}(2z,2\tau) \ := \ \sum_{m\in\xi} e^{i\pi {}^t m \frac{\tau}{2} m} e^{2i\pi {}^t m z}. \tag{7.1}$$

Note that one has the equalities:

$$\theta_{[0]}(z,\tau) = \theta(2z,2\tau) \quad \text{and} \quad \sum_{\xi\in\mathbb{Z}^g/2\mathbb{Z}^g} \theta_{[\xi]}(z,\tau) = \theta(z,\tau/2).$$

7.2 Addition and isogeny formulas

We now state the formulas that extend the addition, the isogeny formulas in Section 4.3.

Addition formula. We begin by the extension of the addition formula.

Lemma 7.1. *For all a,b,z,w in $\mathbb{C}^g$, $\tau\in\mathcal{H}_g$, one has*

$$\theta_\tau\begin{bmatrix} a+b \\ z+w \end{bmatrix}\theta_\tau\begin{bmatrix} a-b \\ z-w \end{bmatrix} \quad = \quad \sum_{\xi\in\mathbb{Z}^g/2\mathbb{Z}^g} \theta_{2\tau}\begin{bmatrix} a+\xi/2 \\ 2z \end{bmatrix}\theta_{2\tau}\begin{bmatrix} b+\xi/2 \\ 2w \end{bmatrix}. \tag{7.2}$$

Proof. Just write the left-hand side as a double sum over m, n in $\mathbb{Z}^g$ and write $m=(p+\xi/2)+(q+\xi/2)$ and $n=(p+\xi/2)-(q+\xi/2)$ where p and q are in $\mathbb{Z}^g$ and where the k^{th} coordinates of ξ is 0 or 1 according to the parity of m_k-n_k. This gives

$$\begin{aligned} LHS &= \sum_{m,n} e^{i\pi(m+a+b)^2\tau} e^{2i\pi(m+a+b)(z+w)} e^{i\pi(n+a-b)^2\tau} e^{2i\pi(n+a-b)(z-w)}, \\ &= \sum_{\xi,p,q} e^{2i\pi(p+a+\xi/2)^2\tau} e^{4i\pi(p+a+\xi/2)z} e^{2i\pi(q+b+\xi/2)^2\tau} e^{4i\pi(q+b+\xi/2)w} \\ &= \sum_{\xi} \theta_{2\tau}\begin{bmatrix} a+\xi/2 \\ 2z \end{bmatrix}\theta_{2\tau}\begin{bmatrix} b+\xi/2 \\ 2w \end{bmatrix}, \end{aligned}$$

where the sum is over ξ in $\mathbb{Z}^g/2\mathbb{Z}^g$ and hence has 2^g terms. □

When $a = b = 0$, one gets the following corollary.

Corollary 7.2. *For all z, w in $\mathbb{C}^g$, $\tau \in \mathcal{H}_g$, one has*

$$\theta(z+w,\tau)\,\theta(z-w,\tau) \;=\; \sum_{\xi\in\mathbb{Z}^g/2\mathbb{Z}^g} \theta_{[\xi]}(w,\tau)\,\theta_{[\xi]}(z,\tau). \tag{7.3}$$

Isogeny formula. We now explain the extension of the isogeny formula.

Lemma 7.3. *Let $\tau \in \mathcal{H}_g$ and $\mathbf{d} \in \mathcal{M}(g,\mathbb{Z})$ with non zero determinant. Set $G_{\mathbf{d}} := {}^t\mathbf{d}^{-1}\mathbb{Z}^g/\mathbb{Z}^g$. Then, one has*

$$\sum_{\ell\in G_{\mathbf{d}}} \theta(\ell,\tau) \;=\; |G_{\mathbf{d}}|\;\theta(0,{}^t\mathbf{d}\tau\mathbf{d}).$$

Proof. Just write the left-hand side LHS as a double sum over m in $\mathbb{Z}^g$ and ℓ in $G_{\mathbf{d}}$ and notice that $\sum_{\ell\in G_{\mathbf{d}}} e^{2i\pi{}^tm\ell}$ is equal to the order $|G_{\mathbf{d}}|$ of the group $G_{\mathbf{d}}$ when m belongs to $\mathbf{d}\,\mathbb{Z}^g$ and is equal to 0 otherwise. Hence

$$LHS \;=\; |G_{\mathbf{d}}| \sum_{m\in\mathbf{d}\mathbb{Z}^g} e^{i\pi{}^tm\tau m} \;=\; |G_{\mathbf{d}}|\;\theta(0,{}^t\mathbf{d}\tau\mathbf{d}).$$

This proves our claim. □

Corollary 7.4. *Let $\tau \in \mathcal{H}_g$ and $\mathbf{d} \in \mathcal{M}(g,\mathbb{Z})$ with $\mathbf{d} \equiv \mathbf{1}$ mod 2. Set $G_{\mathbf{d}} := {}^t\mathbf{d}^{-1}\mathbb{Z}^g/\mathbb{Z}^g$. Then for all $\xi \in \mathbb{Z}^g/2\mathbb{Z}^g$, one has*

$$\sum_{\ell\in G_{\mathbf{d}}} \theta_{[\xi]}(\ell,\tau) \;=\; |G_{\mathbf{d}}|\;\theta_{[\xi]}(0,{}^t\mathbf{d}\tau\mathbf{d}).$$

The proof is very similar. The assumption $\mathbf{d} \equiv \mathbf{1}$ mod 2 is useful to keep track of the cosets ξ by writing $\mathbf{d}\mathbb{Z}^g \cap \xi = \mathbf{d}(\mathbb{Z}^g \cap \xi)$.

7.3 The transformation formula

We now explain the extension of the transformation formula in Section 4.4. We state it up to sign for the theta functions with characteristic. It deals with an element $\sigma = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{Sp}(g,\mathbb{Z})$. This formula is particularly simple when σ belongs to the theta group and when it is expressed with the *modified* theta function

$$\widetilde{\theta}_\tau\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right] \;=\; e^{-i\pi{}^tab}\,\theta_\tau\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right]. \tag{7.4}$$

Note that there is no *modification* when $b = 0$.

The following subgroups of the integral symplectic group $\mathrm{Sp}(g, \mathbb{Z}) := \mathrm{GL}(2g, \mathbb{Z}) \cap \mathrm{Sp}(g, \mathbb{R})$, analogs of (6.7) and (6.8), will play an important role in the transformation formula of the theta functions. The first one is the *integral congruence symplectic group* $\mathrm{Sp}^2_{g,\mathbb{Z}}$ *of level* 2.

$$\mathrm{Sp}^2_{g,\mathbb{Z}} := \mathrm{Sp}(g, \mathbb{Z}) \cap \mathrm{Sp}^2_{g,\mathbb{Q}}.$$

The second one is the *integral symplectic theta group* $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Z}}$ *of level* 2*.*

$$\mathrm{Sp}^{\theta,2}_{g,\mathbb{Z}} := \mathrm{Sp}(g, \mathbb{Z}) \cap \mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}.$$

This group is sometimes called the *Igusa group of level* 2. We also define the *integral symplectic theta subgroup of level* 1

$$\mathrm{Sp}^{\theta}_{g,\mathbb{Z}} := \{h = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Sp}_{g,\mathbb{Z}} \mid ({}^t\alpha\gamma)_0 \equiv ({}^t\beta\delta)_0 \equiv 0 \bmod 2\},$$

Lemma 7.5. *Let $\tau \in \mathcal{H}_g$ and $\sigma \in \mathrm{Sp}^{\theta}_{g,\mathbb{Z}}$. Then, for a, b in $\mathbb{C}^g$, one has*

$$\begin{aligned} \widetilde{\theta}_{\sigma\tau}\left[\begin{smallmatrix} \delta a - \gamma b \\ -\beta a + \alpha b \end{smallmatrix}\right] &= j(\sigma, \tau)\ \widetilde{\theta}_{\tau}\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right], \text{ where} && (7.5) \\ j(\sigma, \tau) &= \kappa(\sigma) \det_{\mathbb{C}}(\gamma\tau + \delta)^{\frac{1}{2}} && (7.6) \end{aligned}$$

This formula is easily remembered if one notices that

$$\left[\begin{smallmatrix} \delta a - \gamma b \\ -\beta a + \alpha b \end{smallmatrix}\right] = {}^t\sigma^{-1}\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right].$$

In this formula, $j(\sigma, \tau)$ is a cocycle on $\mathrm{Sp}^{\theta}_{g,\mathbb{Z}} \times \mathcal{H}_g$ called the *theta cocycle* which is analytic in τ: one has

$$j(\sigma_1\sigma_2, \tau) = j(\sigma_1, \sigma_2\tau)\, j(\sigma_2, \tau).$$

The constant $\kappa(\sigma)$ is a eighth root of unity, $\kappa(\sigma)^8 = 1$, that depends only on σ. The square root $\det_{\mathbb{C}}(\gamma\tau + \delta)^{\frac{1}{2}}$ of the complex number $\det_{\mathbb{C}}(\gamma\tau + \delta)$. To avoid heavy notations we will not explain here the sign issue.

Proof. See [14, Section 8.6 p.231]. One proves a more involved transformation formula for $\theta_{\sigma\tau}\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ valid for all σ in $\mathrm{Sp}(g, \mathbb{Z})$, by checking it on generators of $\mathrm{Sp}(g, \mathbb{Z})$. The first generators are translations by an integral symmetric matrix β,

$$\theta_{\tau+\beta}\left[\begin{smallmatrix} a \\ -\beta a + b + \beta_0/2 \end{smallmatrix}\right] = e^{i\pi {}^t a(-\beta a + \beta_0)}\ \theta_{\tau}\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right], \tag{7.7}$$

where β_0 is the diagonal of β seen as an element of $\mathbb{Z}^g$.

The formula for the second generator is the Poisson formula,

$$\theta_{-\tau^{-1}}\begin{bmatrix}-b\\ a\end{bmatrix} = \det{}_{\mathbb{C}}(-i\tau)^{\frac{1}{2}}\, e^{-2i\pi{}^tab}\,\theta_\tau\begin{bmatrix}a\\ b\end{bmatrix}, \tag{7.8}$$

where the square root is defined by holomorphic continuation in τ with the constraint that when $\tau = i\mathbf{1}$ it is equal to 1. One uses then the fact that the map $(\sigma, \tau) \mapsto \det_{\mathbb{C}}(\sigma\tau + \delta)$ is a cocycle on $\mathrm{Sp}(g, \mathbb{Z}) \times \mathcal{H}_g$. □

The following corollary of Lemma 7.5 is due to Igusa.

Corollary 7.6. *When $\sigma \in \mathrm{Sp}^{\theta,2}_{g,\mathbb{Z}}$ and $\tau \in \mathcal{H}_g$, the ratios $\frac{\theta_{[\xi]}(0,\sigma\tau)}{\theta_{[\xi]}(0,\tau)}$ do not depend on $\xi \in \mathbb{Z}^g/2\mathbb{Z}^g$.*

One can prove that both vectors $(\theta_{[\xi]}(0,\tau)_{\xi\in\mathbb{Z}^g/2\mathbb{Z}^g}$ and $(\theta_{[\xi]}(0,\sigma\tau)_{\xi\in\mathbb{Z}^g/2\mathbb{Z}^g}$ are non zero. Hence they both define a point in the projective space $\mathbb{P}(\mathbb{C}^{2^g})$ and Corollary 7.6 expresses the equality between these two points.

Proof of Corollary 7.6. Introduce $\sigma' := \begin{pmatrix}\alpha & 2\beta\\ \gamma/2 & \delta\end{pmatrix}$ so that $\sigma'(2\tau) = 2\sigma\tau$. Since the matrix σ is in $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Z}}$, the matrix σ' is in $\mathrm{Sp}^{\theta}_{g,\mathbb{Z}}$. We claim that, for all $\xi \in \mathbb{Z}^g/2\mathbb{Z}^g$,

$$\theta_{[\xi]}(0,\sigma\tau) \;=\; j(\sigma', 2\tau)\,\theta_{[\xi]}(0,\tau). \tag{7.9}$$

Indeed, we compute remembering that, by assumption, the matrices $(\delta-1)/2$, $\beta/2$, the vector ξ and the scalar ${}^t\xi{}^t\delta\beta\xi/4$ are all integral,

$$\theta_{[\xi]}(0,\sigma\tau) \;=\; \theta_{\sigma'(2\tau)}\begin{bmatrix}\xi/2\\ 0\end{bmatrix} \;=\; \theta_{\sigma'(2\tau)}\begin{bmatrix}\delta\xi/2\\ -\beta\xi\end{bmatrix} \;=\; \widetilde{\theta}_{\sigma'(2\tau)}\begin{bmatrix}\delta\xi/2\\ -\beta\xi\end{bmatrix}$$

We now apply the transformation formula in Lemma 7.5 to the pair $(\sigma', 2\tau)$,

$$\theta_{[\xi]}(0,\sigma\tau) \;=\; j(\sigma', 2\tau)\,\widetilde{\theta}_{2\tau}\begin{bmatrix}\xi/2\\ 0\end{bmatrix} \;=\; j(\sigma', 2\tau)\,\theta_{2\tau}\begin{bmatrix}\xi/2\\ 0\end{bmatrix} \;=\; j(\sigma', 2\tau)\,\theta_{[\xi]}(0,\tau).$$

This proves that the ratio $\dfrac{\theta_{[\xi]}(0,\sigma\tau)}{\theta_{[\xi]}(0,\tau)}$ does not depend on ξ as required. □

7.4 Construction of critical values

We can now explain the construction of critical functions. The construction involves a matrix $\mathbf{d}$ with integer coefficients and $\det(\mathbf{d}) \neq 0$, and its associate group $G_{\mathbf{d}} := {}^t\mathbf{d}^{-1}\mathbb{Z}^g/\mathbb{Z}^g$ whose order $|G_{\mathbf{d}}|$ is equal to $|\det(\mathbf{d})|$. In this lecture, we will choose $\mathbf{d} = \mathrm{diag}(d_1, ..., d_g)$ where each coefficient is positive and divides the next one: $d_1|d_2|\cdots|d_g$. Note that any finite abelian group is isomorphic to a unique group $G_{\mathbf{d}}$ with such a diagonal matrix $\mathbf{d}$. This group $G_{\mathbf{d}}$ is cyclic of order d if and only if $1 = d_1 = \cdots = d_{g-1} \leqslant d_g = d$.

Theorem 7.7. *Let $\tau \in \mathcal{H}_g$ and $\mathbf{d} \in \mathcal{M}(g, \mathbb{Z})$ with $\mathbf{d} \equiv \mathbf{1} \bmod 2$.*
Assume that there exists $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Sp}^{\theta,2}_{g,\mathbb{Z}}$ such that $\sigma\tau = {}^t\mathbf{d}\tau\mathbf{d}$.
a) There exists $\lambda \in \mathbb{C}$ such that, for all z in $\mathbb{C}^g$, the function
$f_{z,\tau} : \ell \mapsto \theta_\tau(z+\ell)$ is λ-critical on the group $G_{\mathbf{d}} := {}^t\mathbf{d}^{-1}\mathbb{Z}^g/\mathbb{Z}^g$.
b) One has $\lambda = \kappa \det_{\mathbb{C}}(\gamma\tau + \delta)^{1/2}|G_{\mathbf{d}}|$, where $\kappa^8 = 1$.

One can determine the 8th root of unity κ up to sign by using Proposition 5.4 which says that $\frac{\lambda-1}{2}$ is an algebraic integer. Indeed, the only 8th roots of unity κ with $\frac{\kappa-1}{2}$ algebraic integer are $\kappa = \pm 1$.

Proof of Theorem 7.7. The strategy is exactly the same as in dimension $g = 1$. We want to check that, for all z in $\mathbb{C}^g$,

$$\sum_{\ell \in G_{\mathbf{d}}} \theta(z+\ell, \tau)\, \theta(z-\ell, \tau) \;=\; \lambda\, \theta(z, \tau)^2.$$

For w in $\mathbb{C}^g$ we introduce the function on $\mathbb{C}^g$

$$z \mapsto F_w(z) = F_w(z, \tau) := \theta(z+w, \tau)\, \theta(z-w, \tau).$$

We want to know when the two functions $\sum_{\ell \in G_{\mathbf{d}}} F_\ell$ and $F_0 = \theta^2$ are proportional. The key point in the proof is that all these functions F_w live in a finite dimensional vector space with a convenient basis: $(\theta_{[\xi]})_{\xi \in \mathbb{Z}^g/2\mathbb{Z}^g}$. We only have to express that the coefficients of our two functions in this basis are proportional. These coefficients are given by the following calculation in which we apply successively the addition formula and the isogeny formula,

$$\begin{aligned} \sum_{\ell \in G_{\mathbf{d}}} F_\ell(z, \tau) \;&=\; \sum_{\ell \in G_{\mathbf{d}}} \sum_{\xi \in \mathbb{Z}^g/2\mathbb{Z}^g} \theta_{[\xi]}(\ell, \tau)\, \theta_{[\xi]}(z, \tau) \\ &=\; |G_{\mathbf{d}}| \sum_{\xi \in \mathbb{Z}^g/2\mathbb{Z}^g} \theta_{[\xi]}(0, {}^t\mathbf{d}\tau\mathbf{d})\, \theta_{[\xi]}(z, \tau) \quad \text{and} \end{aligned}$$

$$\theta(z,\tau)^2 \;=\; \sum_{\xi\in\mathbb{Z}^g/2\mathbb{Z}^g} \theta_{[\xi]}(0,\tau)\,\theta_{[\xi]}(z,\tau).$$

These two functions are proportional with proportionality factor λ if and only if one has,

$$\lambda = |G_{\mathbf{d}}|\,\frac{\theta_{[\xi]}(0,{}^t\mathbf{d}\tau\mathbf{d})}{\theta_{[\xi]}(0,\tau)}, \qquad \text{for all } \xi \text{ in } \mathbb{Z}^g/2\mathbb{Z}^g. \tag{7.10}$$

By assumption one has ${}^t\mathbf{d}\tau\mathbf{d} = \sigma\tau$ with $\sigma \in \mathrm{Sp}^{\theta,2}_{g,\mathbb{Z}}$, therefore, by Corollary 7.6, these ratios do not depend on $\xi \in \mathbb{Z}^g/2\mathbb{Z}^g$ and are equal to

$$\lambda \;=\; j(\sigma',2\tau)\,|G_{\mathbf{d}}| \;=\; \kappa(\sigma')\,\det_{\mathbb{C}}(\gamma\tau+\delta)^{1/2}\,|G_{\mathbf{d}}|\,, \tag{7.11}$$

where the matrix $\sigma' := \left(\begin{smallmatrix}\alpha & 2\beta\\ \gamma/2 & \delta\end{smallmatrix}\right)$ belongs to $\mathrm{Sp}^{\theta}_{g,\mathbb{Z}}$ and $\kappa(\sigma')^8 = 1$. □

7.5 The symplectic adapted basis

In this section we discuss the structure of the *rational symplectic group* $\mathrm{Sp}(g,\mathbb{Q}) := \mathrm{GL}(2g,\mathbb{Q}) \cap \mathrm{Sp}(g,\mathbb{R})$, and its relation with the *integral symplectic group* $\mathrm{Sp}(g,\mathbb{Z})$.

Proposition 7.8. *Let $h \in \mathrm{Sp}(g,\mathbb{Q})$. Then there exists σ_1 and σ_2 in $\mathrm{Sp}(g,\mathbb{Z})$ and a diagonal matrix $\mathbf{d} = \mathrm{diag}(d_1,\dots,d_g)$ with $d_1|d_2|\dots|d_g$ integral and*

$$h \;=\; \sigma_1 \begin{pmatrix} {}^t\mathbf{d}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{d} \end{pmatrix} \sigma_2.$$

Proposition 7.8 follows from the following proposition. This proposition is a variation of the "adapted basis theorem" which takes into account the existence of a symplectic form. We introduce the set $\mathcal{M}p(n,\mathbb{Z})$ of nonzero integral matrices which are proportional to elements of $\mathrm{Sp}(n,\mathbb{R})$,

$$\mathcal{M}p(n,\mathbb{Z}) := \{g \in \mathcal{M}(2n,\mathbb{Z}) \mid {}^tgJg = \lambda^2 J \text{ for some } \lambda \text{ in } \mathbb{R}^*\}.$$

Proposition 7.9. *Let $g \in \mathcal{M}p(n,\mathbb{Z})$. Then there exist two matrices σ and σ' in $\mathrm{Sp}(n,\mathbb{Z})$ and a positive integral diagonal matrix $\mathbf{a} = \mathrm{diag}(a_1,\dots,a_{2n})$ with $a_1|a_2|\dots|a_n$, with $a_n|a_{2n}$ and such that*

$$g \;=\; \sigma\,\mathbf{a}\,\sigma'.$$

Note that the matrix $\mathbf{a}$ is also in $\mathcal{M}p(n, \mathbb{Z})$ and hence the products $a_j a_{n+j}$ do not depend on the positive integer $j \leqslant n$. Indeed it is equal to λ^2. In particular, one has $a_{2n}|a_{2n-1}|\ldots|a_{n+1}$.

We first recall the well-known undergraduate "adapted basis theorem" for $\mathbb{Z}$-modules or, equivalently, the "Smith normal form" for integral matrices.

Proposition 7.10. (Smith) *Let $g \in \mathcal{M}(n, \mathbb{Z})$. Then there exist σ and σ' in $\mathrm{SL}(n, \mathbb{Z})$ and an integral diagonal matrix $\mathbf{a} = \mathrm{diag}(a_1, \ldots, a_n)$ with $a_1|a_2|\ldots|a_n$, and such that*

$$g = \sigma \, \mathbf{a} \, \sigma'. \tag{7.12}$$

For the proof of Proposition 7.9, we need the following lemma. We recall that a nonzero vector v of $\mathbb{Z}^k$ is primitive if it spans the $\mathbb{Z}$-module $\mathbb{R}v \cap \mathbb{Z}^k$.

Lemma 7.11. *The group $\mathrm{Sp}(n, \mathbb{Z})$ acts transitively on the set of primitive vectors in $\mathbb{Z}^{2n}$.*

Denote by $f_1, \ldots, f_n, e_1, \ldots, e_n$ the canonical basis of $\mathbb{Z}^{2n}$ so that our symplectic form is $\omega = f_1^* \wedge e_1^* + \cdots + f_n^* \wedge e_n^*$.

Proof of Lemma 7.11. Let $v = (x_1, .., x_{2n})$ be a primitive vector in $\mathbb{Z}^{2n}$. We want to find $\sigma \in \mathrm{Sp}(n, \mathbb{Z})$ such that $\sigma v = e_1$.

This is true for $n = 1$. Using the subgroups $\mathrm{Sp}(1, \mathbb{Z})$ for the planes $\mathbb{Z}e_j \oplus \mathbb{Z}f_j$, with $j = 1, \ldots, n$, we can assume that

$$x_{n+1} = \cdots = x_{2n} = 0.$$

In this case the vector $(x_1, \ldots, x_n)$ is primitive in $\mathbb{Z}^n$.

Since $\mathrm{SL}(n, \mathbb{Z})$ acts transitively on the set of primitive vectors in $\mathbb{Z}^n$, we can find a block diagonal matrix $\sigma = \mathrm{diag}(\sigma_0, {}^t\sigma_0^{-1})$, with $\sigma_0 \in \mathrm{SL}(n, \mathbb{Z})$ such that $\sigma v = e_1$. This matrix σ belongs to $\mathrm{Sp}(n, \mathbb{Z})$. □

Proof of Proposition 7.9. Set $\Gamma := \mathrm{Sp}(n, \mathbb{Z})$. The proof is by induction on n. It relies on a succession of steps, in the spirit of the Smith normal form, in which one multiplies on the right or on the left the matrix g by an "elementary" matrix to obtain a simpler matrix $g' \in \Gamma g \Gamma$. We have to pay attention that at each step the elementary matrix is symplectic.

We can assume that the gcd of the coefficients of g is equal to 1. We denote by λ the positive real factor such that g/λ belongs to $\mathrm{Sp}(n, \mathbb{R})$. Note that λ^2 is a positive integer. At the end of the proof we will see that $a_1 = 1$ and $a_{n+1} = \lambda^2$.

1^{st} step: *We find $g' \in \Gamma g \Gamma$ such that $g'e_1 = e_1$.*

Since the coefficients of the integral matrix g are relatively prime, by Proposition 7.10, there exists a primitive vector v in $\mathbb{Z}^{2n}$ such that gv is also primitive. Indeed, by Proposition 7.10, one can write $g = \sigma_o \mathbf{a}_o \sigma'_o$ with σ_o and σ'_o in $\mathrm{SL}(n, \mathbb{Z})$ and $\mathbf{a}_o = \mathrm{diag}(a_{o,1}, \ldots, a_{o,2n})$ with $1 = a_{o,1}|a_{o,2}| \ldots |a_{o,2n}$. One can then choose $v = {\sigma'_o}^{-1} e_1$ so that $gv = \sigma_o e_1$.

Then, according to lemma 7.11, there exists σ, σ' in Γ such that $\sigma g v = e_1$ and $\sigma' e_1 = v$. Then the matrix $g' := \sigma g \sigma'$ satisfies $g'e_1 = e_1$.

2^{nd} step: *We find $g' \in \Gamma g \Gamma$ with $g'e_1 = e_1$* and *$\omega(f_1, g'e_j) = 0$ for $j > 1$.*

By the first step, we can assume that

$$g \;=\; \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \text{ with } \alpha e_1 = e_1 \text{ and } \gamma e_1 = 0$$

In particular the first column of the integral matrix α is $(1, 0, \ldots, 0)$. We would like the first row of α to be also of the form $(1, 0, \ldots, 0)$. For that we choose $g' = g\sigma'$ where σ' is the symplectic transformation

$$\sigma' = \mathbf{1}_n + \textstyle\sum_{1<j\leqslant n} \alpha_{1,j} (f_j \otimes f_1^* - e_1 \otimes e_j^*) \in \mathrm{Sp}(n, \mathbb{Z}),$$

in which the integers $\alpha_{1,j}$ are the coefficients of the first row of the matrix α.

3^{rd} step: *We find $g' \in \Gamma g \Gamma$ such that $g'e_1 = e_1$ and $g'f_1 = \lambda^2 f_1$.*

By the second step, we can assume, writing $g = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ that both the first row and first column of α are $(1, 0, \ldots, 0)$, and the first column of γ is $(0, \ldots, 0)$. We would also like the first row of β to be $(0, \ldots, 0)$. For that we choose $g' = g\sigma'$ where σ' is the symplectic transformation

$$\sigma' = \mathbf{1}_n - \beta_{1,1} e_1 \otimes f_1^* - \textstyle\sum_{1<j\leqslant n} \beta_{1,j} (e_j \otimes f_1^* + e_1 \otimes f_j^*) \in \mathrm{Sp}(n, \mathbb{Z}).$$

Now by construction one has

$$\begin{array}{rcl} \omega(f_1, g'e_j) & = & 0 \quad \text{for } 1 < j \leqslant n, \\ \omega(f_1, g'e_1) & = & 1 \;\text{ and} \\ \omega(f_1, g'f_j) & = & 0 \quad \text{for } j \leqslant n. \end{array}$$

Since g'/λ is symplectic, this implies that $g'^{-1}f_1 = \lambda^{-2}f_1$, or equivalently, $g'f_1 = \lambda^2 f_1$ as required.

4$^{\text{th}}$ step: *Conclusion.*

By the third step, we can assume that $ge_1 = e_1$ and $gf_1 = \lambda^2 f_1$. Therefore g preserves the symplectic $\mathbb{Z}$-submodule of $\mathbb{Z}^{2n}$ orthogonal of $\mathbb{Z}f_1 \oplus \mathbb{Z}e_1$, which admits $f_2, \ldots, f_n, e_2, \ldots, e_n$ as $\mathbb{Z}$-basis. We conclude by applying the induction hypothesis to the restriction $g' \in \mathcal{M}p(n-1, \mathbb{Z})$ of g to this $\mathbb{Z}$-module. □

Recall the *rational congruence symplectic group* $\mathrm{Sp}^{\ell}_{g,\mathbb{Q}}$ *of level* ℓ and the *rational symplectic theta group* $\mathrm{Sp}^{\theta,\ell}_{g,\mathbb{Q}}$ *of level* ℓ introduced in (6.7) and (6.8).

Lemma 7.12. *Let* $h \in \mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$ *and write* $h = \sigma_1 \left(\begin{smallmatrix} {}^t\mathbf{d}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{d} \end{smallmatrix}\right)\sigma_2$ *with* $\mathbf{d}$ *in* $\mathcal{M}(g, \mathbb{Z})$ *and both* σ_1, σ_2 *in* $\mathrm{Sp}(g, \mathbb{Z})$. *Then* $\det(\mathbf{d})$ *is odd and* $\sigma_2\sigma_1$ *is in* $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Z}}$.

Proof of Lemma 7.12. The group $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$ is a normal subgroup of $\mathrm{Sp}(g, \mathbb{Z}_{(2)})$. Since the element h belongs to $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$, the conjugate

$$h' := \sigma_1^{-1} h \sigma_1 = \left(\begin{smallmatrix} {}^t\mathbf{d}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{d} \end{smallmatrix}\right)\sigma_2\sigma_1$$

also belongs to $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$. Therefore the determinant $\det(\mathbf{d})$ is odd and the product $\sigma_2\sigma_1$ is in $\mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$. □

7.6 Unitary endomorphism of abelian varieties

Proof of Theorem 6.19. The key point is the interrelation between the tangent map T_ν and the holonomy h_ν, together with the use of Proposition 7.8. We fix a symplectic $\mathbb{Z}$-basis $(f_1, \ldots, f_g, e_1, \ldots, e_g)$ of Λ so that $\omega = \sum f_j^* \wedge e_j^*$.

Let $\sigma_\nu = \left(\begin{smallmatrix} \alpha_\nu & \beta_\nu \\ \gamma_\nu & \delta_\nu \end{smallmatrix}\right) \in \mathrm{Sp}^{\theta,2}_{g,\mathbb{Q}}$ such that ${}^t\sigma_\nu$ is the matrix of h_ν in the symplectic basis $(f_1, \ldots, f_g, e_1, \ldots, e_g)$.

This means that one has the equality in V^{2g}

$$(T_\nu f_1, \ldots, T_\nu f_g, T_\nu e_1, \ldots, T_\nu e_g) = (f_1, \ldots, f_g, e_1, \ldots, e_g)\, {}^t\sigma_\nu. \tag{7.13}$$

We introduce the Riemann matrix $\tau_\nu \in \mathcal{H}_g$ such that

$$\begin{aligned} (f_1, \dots, f_g) &= (e_1, \dots, e_g)\tau_\nu \text{ and hence} \\ (T_\nu f_1, \dots, T_\nu f_g) &= (T_\nu e_1, \dots, T_\nu e_g)\tau_\nu, \end{aligned} \tag{7.14}$$

one has

$$\sigma_\nu \tau_\nu = \tau_\nu. \tag{7.15}$$

By the adapted symplectic basis in Proposition 7.8, there exist σ_1, σ_2 in $\mathrm{Sp}(g, \mathbb{Z})$ and an integral matrix $\mathbf{d}$ with $\det(\mathbf{d}) \neq 0$ such that

$$\sigma_\nu = \sigma_1 \, D \sigma_2 \ \text{ with } \ D := \left(\begin{smallmatrix} {}^t\mathbf{d}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{d} \end{smallmatrix}\right). \tag{7.16}$$

The matrix $\mathbf{d}$ can be chosen to be a diagonal matrix $\mathrm{diag}(d_1, \dots, d_g)$ with positive integer coefficients $d_1|d_2|\dots|d_g$.

Let $\tau := \sigma_1^{-1}\tau_\nu$ and $\sigma = \sigma_2\sigma_1$ so that Equation (7.15) can be re written

$${}^t\mathbf{d}\tau\mathbf{d} = D^{-1}\sigma_1^{-1}\tau_\nu = \sigma_2\sigma_\nu^{-1}\tau_\nu = \sigma_2\tau_\nu = \sigma\tau. \tag{7.17}$$

Since σ_ν preserves a theta structure of level 2, by Lemma 7.12, the symplectic matrix $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ belongs to $\mathrm{Sp}_{g,\mathbb{Z}}^{\theta,2}$. Therefore by Theorem 7.7, the value

$$\lambda_\nu = \kappa \det\nolimits_{\mathbb{C}}(\gamma\tau + \delta)^{1/2} |\det(\mathbf{d})| \tag{7.18}$$

is critical on the group $G_{\mathbf{d}} \simeq G_\nu$, where κ is a 8th root of unity.

It only remains to check that this value (7.18) is equal to (6.9). Using (7.13) and (7.14), we compute

$$(T_\nu e_1, \dots, T_\nu e_g) = (e_1, \dots, e_g)\,(\tau_\nu\, {}^t\gamma_\nu + {}^t\delta_\nu) \quad \text{and}$$

$$\det\nolimits_{\mathbb{C}}(T_\nu) \ = \ \det\nolimits_{\mathbb{C}}(\tau_\nu {}^t\gamma_\nu + {}^t\delta_\nu) = \det\nolimits_{\mathbb{C}}(\gamma_\nu\tau_\nu + \delta_\nu).$$

We go on using the cocycle $c(\sigma, \tau) = \det_{\mathbb{C}}(\gamma\tau + \delta)$ on $\mathrm{Sp}(g, \mathbb{R}) \times \mathcal{H}_g$,

$$\begin{aligned} \det\nolimits_{\mathbb{C}}(T_\nu) &= c(\sigma_\nu, \tau_\nu) = c(D\sigma, \tau) = \det\nolimits_{\mathbb{C}}(\mathbf{d}\gamma\tau + \mathbf{d}\delta) \\ &= \det(\mathbf{d}) \det\nolimits_{\mathbb{C}}(\gamma\tau + \delta)\,. \end{aligned}$$

Plugging this into (7.18), we obtain the equality $\lambda_\nu = \kappa' \, d_\nu^{1/2} \det_{\mathbb{C}}(T_\nu)^{1/2}$. □

7.7 One example using CM number fields

I would like to end this lecture by explaining on one example a method for constructing a principally polarized abelian variety together with a unitary $\mathbb{Q}$-endomorphism ν that give rise to a new critical value. The idea is to specialize our general construction by using a CM number field. This is a totally complex number field K that is a quadratic extensions of a totally real number field K_0.
The method is general but explaining it on one example is more enlighting.

Lemma 7.13. *The value* $\lambda = 1+4\sqrt{2}+2i\sqrt{6-2\sqrt{2}}$ *is up to sign* 57*-critical.*

Proof of Lemma 7.13. One key point is the factorization

$$\lambda = (1+2i\sqrt{3+\sqrt{7}})(1-2i\sqrt{3-\sqrt{7}}). \tag{7.19}$$

⋆ **The number field.** We start with the CM number field $K = \mathbb{Q}[\alpha]$ with $\alpha = i\sqrt{3+\sqrt{7}}$. This field K is a quadratic extension of the real quadratic field $K_0 := \mathbb{Q}[\delta]$ where $\delta := \sqrt{7}$. Its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\alpha]$. We denote by $x \mapsto \check{x}$ the non-trivial field embeddings $\mathbb{K} \to \mathbb{C}$ for which $\check{\alpha} = -i\sqrt{3-\sqrt{7}}$ and hence $\check{\delta} = -\delta$.

⋆ **The complex torus.** We denote by $\Phi : K \to V = \mathbb{C}^2$ the algebra morphism given by $\Phi(x) = (x, \check{x})$. The image $\Lambda := \Phi(\mathcal{O}_K) \subset K$ is a lattice in $\mathbb{C}^2$ and the complex torus will be the quotient $A = \mathbb{C}^2/\Lambda$.

⋆ **The principal polarization.** The symplectic form on Λ is given by a nonzero imaginary element t_0 of K thanks to the simple formula

$$\omega(x, x') = \mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x'}/t_0).$$

A key point is to choose t_0 so that this symplectic form is integral with determinant 1 on Λ and such that both the imaginary part of t_0 and $\check{t_0}$ are positive. A good choice is $t_0 = 4\alpha\delta$. One has $\omega = f_1^* \wedge e_1^* + f_2^* \wedge e_2^*$ in the basis $\mathcal{B} = (f_1, f_2, e_1, e_2)$ of $\mathcal{O}_K \simeq \Lambda$ given by

$$f_1 = \alpha\delta\ ,\ \ f_2 = \alpha\ ,\ \ e_1 = 1\ ,\ \ e_2 = \delta\,.$$

We notice that ω is the restriction to $V_{\mathbb{Q}} = \Phi(K)$ of the imaginary part of the positive hermitian form H on $\mathbb{C}^2$ given by

$$H(z, z') = 2iz_1\overline{z_1'}/t_0 + 2iz_2\overline{z_2'}/\check{t_0}.$$

Then we have checked that the torus $A = \mathbb{C}^2/\Lambda$ is a principally polarized abelian variety.

$\star$ **The unitary $\mathbb{Q}$-endomorphism of A.** The unitary $\mathbb{Q}$-endomorphisms ν are nothing but elements $\nu \in K$ of absolute value 1. One chooses ν of the form $\nu = \frac{\mu}{\overline{\mu}}$ in such a way that $\mu \in 1 + 2\mathcal{O}_K$. We will choose $\mu = 1 + 2\alpha$. The matrix m_μ of multiplication by μ in the basis $\mathcal{B}$ belongs to $\mathcal{M}(4, \mathbb{Z})$, is equal to $\mathbf{1}$ mod 2 and has determinant $\det(m_\mu) = N_{K/\mathbb{Q}}(\mu) = 57$.
Therefore the matrix m_ν belongs to $\mathrm{Sp}^4_{2,\mathbb{Q}}$ and ν preserves a theta structure of level 2.

$\star$ **The finite abelian group.** Since the elements μ and $\overline{\mu}$ are coprime, one has $\mu\mathcal{O}_K \cap \overline{\mu}\mathcal{O}_K = \mu\overline{\mu}\mathcal{O}_K$, and the group $G_\nu = \nu^{-1}\mathcal{O}_K/(\nu^{-1}\mathcal{O}_K \cap \mathcal{O}_K)$ is isomorphic to $\mathcal{O}_K/\mu\mathcal{O}_K$ which has order $d_\nu = N_{K/\mathbb{Q}}(\mu) = 57$ and hence is isomorphic to $\mathbb{Z}/57\mathbb{Z}$.

$\star$ **The critical value.** According to Theorem 6.19, the corresponding critical value $\lambda = \lambda_\nu$ is given by $\lambda_\nu^2 = \kappa^2 d_\nu \nu\check{\nu} = \kappa^2\mu^2\check{\mu}^2$ where $\kappa^8 = 1$. Therefore one has $\lambda_\nu = \kappa\mu\check{\mu}$. We conclude thanks to the factorization (7.19) that $\lambda_\nu = \kappa\lambda$.

$\star$ **The 8th root of unity.** As we explained just after Theorem 6.19, one can determine the 8th root of unity κ up to sign by using Proposition 5.4 which says that $\frac{\lambda_\nu - 1}{2}$ is an algebraic integer. Indeed, the only 8th roots of unity κ with $\frac{\kappa-1}{2}$ algebraic integer are $\kappa = \pm 1$. Therefore, since $\frac{\lambda-1}{2}$ is an algebraic integer, one has $\lambda_\nu = \pm\lambda$. □

Remark 7.14. One can prove that $\lambda_\nu = \lambda$ with a plus sign. But this require extra technical works that can be found in [10]

We get more examples by choosing other CM number fields and other elements $\nu = \frac{\mu}{\overline{\mu}}$ of K with $\mu \in 1 + 2\mathcal{O}_K$. For instance, one can also obtain this way the values (6.1) and (6.2). One can also prove the following proposition.

Proposition 7.15. *Let $K := \mathbb{Q}[e^{2i\pi/n}]$ and $\mu = 1 + s - \overline{s}$ where $s \in \mathcal{O}_K$ with $N_{K/\mathbb{Q}}(\mu)$ odd. Then for all CM types Φ of K, the reflex norm up to sign $\lambda = \pm N_\Phi(\mu)$ is a critical value on the finite abelian group $G = \mathcal{O}_K/\mu\mathcal{O}_K$.*

By definition a CM-type Φ of K is a choice of one embedding ρ for each pair of conjugate embeddings of K in $\mathbb{C}$ and the reflex norm $N_\Phi(\mu)$ is the product of these images $\rho(\mu)$.

Notes to Chapter 7. We followed [10] but used also [18], [14], [35], [12].

The first reference to Proposition 7.8 that I know is Shimura's paper [40, Prop. 1.6]. Moreover in [41], Shimura points out the relevance of this theorem to understand the modular forms on Siegel upper halfspace.

Part III
Equiangular lines

In the last part of this course, we focus on the main topic: The Equiangular Lines. This topic looks very naive at first glance.

The aim of this part is to explain why one expects that the maximal number of equiangular lines in $\mathbb{C}^d$ is d^2 and that such a configuration of equiangular lines called a SIC, is organized in a so nice way that one may call it an equiangular dream.

At first glance this question does not seem to be related to group theory. The main surprise is that many finite groups are crucial in this subject:
⋆ the Heisenberg group H_d over $\mathbb{Z}/d\mathbb{Z}$,
⋆ the projective metaplectic group PM_d which is isomorphic to $\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$,
⋆ the multiplicative group of $(\mathbb{Z}/d\mathbb{Z})[\omega]$ where $\omega^2 + \omega + 1 = 0$,
⋆ the Galois group of abelian extensions of a real quadratic field $\mathbb{K}$,
⋆ the ideal ray class groups of orders $\mathcal{O}' \subset \mathcal{O}_{\mathbb{K}}$ in this field $\mathbb{K}$.

The relationship with the previous lectures is that we are looking at this vector space as the space of functions on a finite abelian group G, in most of the case we will choose $G = \mathbb{Z}/d\mathbb{Z}$. The generators of these d^2 lines will be the images $F^k E^j v_0$ of a well chosen function v_0 on $\mathbb{Z}/d\mathbb{Z}$ where E is the translation operator and F is the operator of multiplication by an additive character of $\mathbb{Z}/d\mathbb{Z}$. Such a vector v_0 will be called a fiducial vector and the corresponding SIC a Heisenberg SIC or HSIC. For $d = 2$ and $d = 3$ it is very easy to describe fiducial vectors. The first non trivial examples are due to Zauner.

There will be no theorem in this Part III. Only conjectures. This makes the last part of this graduate course kind of very special. Indeed, it maybe the case that it will be very quickly obsolete because a few of these conjectures might be quickly solved. In the presentation of these conjectures we will follow almost a chronological order. We will begin by the elementary conjectures due to Zauner that can be understood at an undergraduate level. The conjectures became more and more precise when computer experiments due to Grassl and Scott gave more and more precise insight in the structure of the HSICs from the algebraic number point of view. A first series of conjectures due to Appleby, Flammia, McConnell, Yard can be understood at a graduate level using only Galois theory. The most recent of these conjectures due to Appleby, Flammia, Kopp, Lagarias, can only be understood within class field theory and relates this problem with the longstanding conjecture of Stark dealing with units in abelian extension of real quadratic fields.

The most advanced and recent of these conjectures, sometimes called "Facts in every known cases" in the litterature, eventhough they are very precise, may not yet be stable. They might need slight modifications. What makes them very valuable is the intrinsic beauty and harmony of the conjectures, and that these conjectures might be solved by one of the readers of this course.

In Lecture 8, we begin by surveying the analog problem of equiangular lines over the reals which is also still open but does not have yet any reasonable conjectural answer. We will then focus up to the end on the complex equiangular lines. We prove the d^2 upper bound for the number of equiangular lines. The examples in dimension 2 and 3 are very easy. We will now assume $d \geqslant 4$. We give then explicit examples of HSIC that occur in dimensions 4, 7, 8 and 19.

In Lecture 9, we explain how the first non-trivial HSICs were found, why it is natural to introduce the metaplectic representation to understand them. We will also study the Zauner matrix Z which happens to be very useful in the construction of HSICs and which is most of the time reponsible of the mysterious symmetry of order 3 satisfied by all known SICs.

In Lecture 10 we state the first series of conjectures on the arithmetic of HSICs. We explain that, conjecturally, there exists a real quadratic field $\mathbb{K} = \mathbb{Q}[\sqrt{\Delta_d}]$ with $\Delta_d = (d{+}1)(d{-}3)$ such that the entries of the orthogonal projector on a fiducial vector belong to an abelian extension of $\mathbb{K}$.

In Lecture 11, we describe in detail the "unique" 5-dimension HSIC and we check the conjectures in this case. This can be seen as a nice exercise in Galois theory.

In Lectures 12, we recall the main results of class field theory, which parametrizes the abelian extension of $\mathbb{K}$, we introduce the ray class fields for orders $\mathcal{O}$ of $\mathbb{K}$ and identifies their Galois group with a ray class group of $\mathcal{O}$.

We also explain the conjecture that describes as a ray class field, the field generated by all the entries of all the projectors on the lines of a given HSIC.

In Lecture 13, we explain more Class Field Theory by introducing the Artin map which is an explicit isomorphism between the ideal ray class group and the Galois group. When the vector v_0 is chosen to be Zauner invariant, we also explain that the ray class group should act on the correlations of the corresponding HSIC through the Artin map.

8 Equiangular lines

This lecture deals with the elementary aspects of equiangular lines. We define the SIC, we explain why the expected values for the number of lines in a SIC is $n = d^2$. We also introduce the fiducial lines whose orbit under the Heisenberg group is a SIC. And we present the simplest SIC in dimension $d = 3$, 4, 7 and the Hoggar SIC in dimension 8

We will then state the first naïve conjectures with respect to existence and finiteness of SICs.

8.1 Real equiangular lines

We begin by the analogous problem in a real vector space.

Introduction

Let $\mathbb{R}^d$ be the d-dimensional euclidean space. What is the maximum number n of lines $D_1, \ldots, D_n$ in $\mathbb{R}^d$ for which the angles θ between two of them is constant? Is this configuration of lines unique modulo isometries? What is the value of this angle θ?

For $d = 2$, one has $n = 3$ and $\cos\theta = 1/2$.

Indeed, starting with a regular hexagon in the plane, the three lines are the lines that join the middle of the opposite sides.

For $d = 3$, one has $n = 6$ and $\cos\theta = 1/\sqrt{5}$.

Indeed, starting with a regular dodecahedron in the space, the six lines are the lines that join the center of the opposite faces.

There is no definitive answer to these questions, but there is a nice partial result due to Gerzon in 1970 that we present now.

Theorem 8.1. *(a) One has $n \leqslant d(d+1)/2$.*
(b) If $n = d(d+1)/2$, then one has $\cos\theta = 1/\sqrt{d+2}$ and hence $\tan\theta = \sqrt{d+1}$.
(c) If $n = d(d+1)/2$ and $d > 3$, then d is odd and $d+2$ is a square.

The value $n = d(d+1)/2$ and the value of the angle θ is nice, but unfortunately it is not known if this phenomenon does occur for infinitely many dimensions $d \geqslant 2$.

For $d = 7$, one has $n = 28$ and $\cos\theta = 1/3$,
Indeed, the 28 lines are spanned by the vector $(-3, -3, 1, 1, 1, 1, 1, 1)$ and its images by permutation of coordinates; they stand in the hyperplane $\sum x_k = 0$ in $\mathbb{R}^8$.

For $d = 23$, one has $n = 276$ and $\cos\theta = 1/5$,
Indeed, the 276 lines form an orbit of the simple Conway sporadic group Co_3 in an hyperplane of the Leech lattice Λ in $\mathbb{R}^{24}$. We will not need this example in the sequel, hence we do not give more details.

One can check in all these four examples with $d = 2$, 3, 7 and 23 that the group of isometries of the equiangular configuration acts transitively on the pair of distinct lines of the configuration.

For $d = 47$, it is unknown if $n = d(d+1)/2$.
More precisely it is not known if there exists any other real equiangular configurations of lines with $n = d(d+1)/2$.

Proof of Theorem 8.1. For $j = 1, \ldots, n$, we choose a vector v_j of norm 1 on the line D_j, so that, for $j \neq k$, one has $(v_j|v_k) = \pm\alpha$ where $\alpha := \cos\theta$. We also introduce the orthogonal projectors P_j on the lines D_j. These P_j live in the $d\,(d+1)/2$-dimensional vector space $S^2\mathbb{R}^d$ of symmetric matrices.

(a) The Gram matrix of this family P_j is the $n \times n$ matrix

$$G = (tr(P_jP_k)) = \begin{pmatrix} 1 & & \alpha^2 \\ & \ddots & \\ \alpha^2 & & 1 \end{pmatrix} = (1-\alpha^2)I_n + \alpha^2 J_n$$

where J_n is the rank one $n \times n$ matrix all of whose entries are equal to 1. The eigenvalues of G are $1-\alpha^2$ and $1-\alpha^2+n\alpha^2$. Since these eigenvalues are non zero, the matrix G is invertible and hence the symmetric matrices P_j are linearly independent and one has $n \leqslant d(d+1)/2$.

(b) When $n = d(d+1)/2$, the n matrices $P'_j := dP_j - I_d$ have zero traces and hence they live in a $(n-1)$-dimensional vector space and are linearly dependent and their Gram matrix

$$\begin{aligned} G' = (tr((dP_j - I_d)(dP_k - I_d))) &= \begin{pmatrix} d^2-d & & d^2\alpha^2-d \\ & \ddots & \\ d^2\alpha^2-d & & d^2-d \end{pmatrix} \\ &= d^2(1-\alpha^2)I_n + (d^2\alpha^2-d)J_n \end{aligned}$$

is not invertible. Since the eigenvalues of J_n are 0 and n, one deduces that $d^2(1-\alpha^2)+n(d^2\alpha^2-d)=0$. After simplification, one gets $\alpha^2(d+2)=1$.

(c) If $n=d(d+1)/2$, the Gram matrix of the vectors v_j has the form

$$g=((v_j|v_k))=\begin{pmatrix} 1 & & \pm\alpha \\ & \ddots & \\ \pm\alpha & & 1 \end{pmatrix}.$$

Its kernel has dimension $m\geqslant n-d\geqslant 1$. Hence the matrix

$$a=\frac{1}{\alpha}(I_n-g)=\begin{pmatrix} 0 & & \pm1 \\ & \ddots & \\ \pm1 & & 0 \end{pmatrix}$$

admits $1/\alpha$ as an eigenvalue with multiplicity $m>n/2$ since $d\geqslant 4$. Since the matrix a has integral entries, the eigenvalue $1/\alpha$ is an algebraic number with no other Galois conjugate, hence the number $1/\alpha$ is a rational number. Since the square of this rational number $1/\alpha$ is the integer $d+2$, it has to be an integer and $d+2$ is a square.

The matrix $(I_n+a+J_n)/2$ also has integral entries. Since $m\geqslant 2$, it admits $(1+1/\alpha)/2$ as an eigenvalue. This eigenvalue is an algebraic integer, hence the integer $1/\alpha$ is an odd integer. □

8.2 Complex equiangular lines

We now introduce the complex equiangular lines.

Introduction Eventhough the answer over the real numbers was not clean, it is very natural to ask for the analogous question over the complex numbers and to ask for the maximum number n of lines $D_1,\ldots,D_n$ in the d-dimensional hermitian space $\mathbb{C}^d$ whose pairwise angles θ are all the same. And to ask for the value of this angle θ?

As in the real case, for $j=1,\ldots,n$, we denote by v_j a vector of norm 1 on D_j, so that, for $j\neq k$, one has

$$|\langle v_j|v_k\rangle|^2=\beta \ \text{ where } \ \beta:=\cos^2\theta.$$

We also introduce the hermitian projectors P_j on the lines D_j. Hermitian means that

$$P_j^*=P_j \quad \text{for all } j.$$

They live in the d^2 dimensional real vector space of $d \times d$ complex hermitian matrices.

The condition expressing these are rank one projectors is

$$P_j^2 = P_j \ , \ \ tr(P_j) = 1 \ \text{ for all } j \leqslant n. \tag{8.1}$$

The condition expressing the equiangular condition is

$$tr(P_j P_k) = \beta \ \text{ for all } j \neq k. \tag{8.2}$$

More generally one can look at families $(P_j)_{j \leqslant n}$ of rank one projectors (8.1) in $\mathrm{End}(\mathbb{C}^d)$ satisfying the equiangular condition (8.2) without requesting that they are hermitian. For such a family one has an analog of Theorem 8.1.

Theorem 8.2. *(Delsarte–Goethals–Seidel, 1975) Let $(P_j)_{j \leqslant n}$ be a family of complex rank-one projectors satisfying the equiangular condition* (8.2) *with $\beta \in \mathbb{C}$, $\beta \neq 1$.*
(a) Then, one has $n \leqslant d^2$.
(b) In case $n = d^2$, one has $\beta = 1/(d+1)$.

Equivalently, for P_j hermitian, one has $\cos\theta = \frac{1}{\sqrt{d+1}}$ or $\tan\theta = \sqrt{d}$.

Proof. The proof is the same as for Theorem 8.1, replacing the real vector space of real symmetric matrices by the complex vector space $\mathrm{End}(\mathbb{C}^d)$ of all complex matrices endowed with the non degenerate bilinar form $(A, B) \mapsto tr(AB)$. We shorten the proof by proving simultaneously (a) and (b).

The matrices $P'_j := dP_j - I_d$ have zero traces, hence they live in a vector space of dimension $d^2 - 1$. Their Gram matrix G' is given by

$$\begin{aligned} G' = (tr((dP_j - I_d)(dP_k - I_d))) \ &= \ \begin{pmatrix} d^2 - d & & d^2\beta - d \\ & \ddots & \\ d^2\beta - d & & d^2 - d \end{pmatrix} \\ &= \ d^2(1-\beta) I_n + (d^2\beta - d) J_n. \end{aligned}$$

The eigenvalues of G' are $d^2(1-\beta)$ and $\lambda = d^2(1-\beta) + dn(d^2\beta - d)$. The first eigenvalue $d^2(1-\beta)$ which has multiplicity $n-1$ is non zero. Therefore the rank of the family $(P'_j)_{j \leqslant n}$ is at least $n-1$. This proves the inequality $n \leqslant d^2$.

Moreover, in case of equality $n = d^2$, the family $(P'_j)_{j \leqslant n}$ has rank equal to $n-1$ and the last eigenvalue $\lambda = d^2(1-\beta) + d^2(d^2\beta - d)$ must be equal to 0. After simplification, one gets $(d+1)\beta = 1$. □

Remark 8.3. The main difference between the maximal configuration of equiangular lines over the real numbers and over the complex numbers is that when one knows the absolute value $|\langle v_j|v_k\rangle|$, one knows the scalar product $\langle v_j|v_k\rangle$ up to sign in the real case, but in the complex case, one only knows it up to a complex number of modulus one. There is much more flexibility.

Definition 8.4. *A SIC or a SICPOVM is a family of d^2 hermitian projectors $(P_1, \dots P_{d^2})$ of rank* 1 *of $\mathbb{C}^d$ such that, for all $j \neq k$, $tr(P_jP_k) = 1/(d+1)$.*

The projectors P_j will always be implicitely assumed to be hermitian i.e. satisfying $P_j^* = P_j$, except if we explicitely relax this assumption. We will then say "a non-necessarily hermitian SIC" The interest in considering the non-hermitian projectors comes from the fact that the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which acts on the set of SICs does not always preserve the condition hermitian. We will say more about this later.

Remark 8.5. The term SICPOVM is an acronym for "Symmetric, Informationally Complete, Positive Operator-Valued Measurements". This name reflects the fact that these configurations were found and first studied in depth by the community of Quantum Computer Scientists.

Zauner in his PhD thesis in 1999, relying on exact computer calculations for $d \leqslant 6$, was the first to guess the existence of (hermitian) SICs in all dimensions.

Conjecture 8.6. *(Zauner) For all integers $d \geqslant 2$ there exists an equiangular configuration with d^2 lines in $\mathbb{C}^d$.*

This conjecture is known only for finitely many dimensions d, among them all the dimensions $d \leqslant 180$. We expect to present at least one explicit SIC for each $d \leqslant 8$.

8.3 First examples of SICs

SIC in dimension 2

They are very easy to describe.

We can do it in a geometric way: one has to find 4 lines in $\mathbb{C}^2$, that is 4 points in $\mathbb{CP}^1$ whose pairwise distance is constant. Since $\mathbb{CP}^1$ is a round 2-sphere, these 4 points are the vertices of a regular tetrahedron.

We can do it in an algebraic way: we choose the 4 lines to be generated by the vectors

$$v_{00} = (a, b),\ v_{10} = (b, a),\ v_{01} = (a, -b),\ v_{11} = (-b, a),$$

where $a = 1+i$, $b = 1+\sqrt{3}$. This is a SIC because one can compute the absolute values of the hermitian products

$$2|\mathbf{Re}(a\bar{b})| = 2|\mathbf{Im}(a\bar{b})| = |b|^2 - |a|^2 = (|a|^2 + |b|^2)/\sqrt{3} = 2 + 2\sqrt{3}.$$

This configuration is unique. This SIC is defined over the field $\mathbb{Q}[i, \sqrt{3}]$. Using another unitary basis of $\mathbb{C}^2$ we can also write

$$v_{00} = (\sqrt{3}, 0),\ v_{10} = (1, \sqrt{2}),\ v_{01} = (1, \omega\sqrt{2}),\ v_{11} = (1, \omega^2\sqrt{2}),$$

where $\omega := e^{2i\pi/3}$.

In this case the angle θ is given by $\cos\theta = 1/\sqrt{3}$.

Remark 8.7. The angle φ between the four vertices of a regular tetrahedron $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, $(-1, -1, 1)$ in $\mathbb{R}^3$ is given by $\cos\varphi = -1/3$. It may seem surprising that, since $\cos\varphi = 2\cos^2\theta - 1$, the angle φ is the double of the angle θ. This can be explained by the fact that SU(2) is a double cover of SO(3) and the sphere $\mathbb{CP}^1$ a double cover of the real projective plane $\mathbb{RP}^2$.

SIC in dimension 3

Those SIC are called Hesse SIC. This is the only dimension for which there is a one parameter family of SICs which are not unitarily equivalent.

Here is the construction which depend on a parameter u which is a complex number of modulus $|u| = 1$. The example with $u = 1$. Denote by $\omega := e^{2i\pi/3}$.

The nine lines generated by the vectors

$$\begin{aligned} v_{00} &= (1, u, 0), & v_{10} &= (0, 1, u), & v_{20} &= (u, 0, 1), \\ v_{01} &= (1, u\omega, 0), & v_{11} &= (0, 1, u\omega), & v_{21} &= (u\omega, 0, 1), \\ v_{02} &= (1, u\omega^2, 0), & v_{12} &= (0, 1, u\omega^2), & v_{22} &= (u\omega^2, 0, 1). \end{aligned}$$

These nine lines form a SIC since, for $ij \neq 00$, one has $\|v_{00}\|^2 = 2|\langle v_{00}|v_{ij}\rangle| = 2$. One can show that those are the only possible SIC in dimension 3.

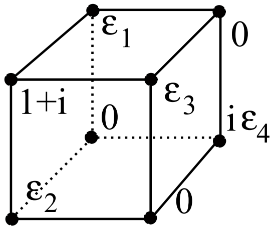
The Hesse SIC with $u = 1$ is rather simple since it is defined over $\mathbb{Q}[\omega]$

Conjecture 8.8. *For $d \geqslant 4$ there exist only finitely many SIC up to a unitary transformation.*

It has been proven by Hughston and Salamon in [24], using ideas from symplectic geometry, that the Hesse SICs are the only hermitian SICs in dimension 3.

SIC in dimension 8
The following SIC in dimension 8 has been found by Hoggar in [23]. He is particularly striking due to the fact that it is the only known SIC which is defined over the field $\mathbb{Q}[i]$. Here is the construction of the Hoggar SIC for $d = 8$. It is defined on the space $\mathbb{C}^8 = \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^3]$.

We identify $(\mathbb{Z}/2\mathbb{Z})^3$ with the vertices of the cube and the space $\mathbb{C}^8$ with the space of functions on the vertices of this cube. The 64 lines that form the SIC are those generated by the 64 functions drawn here where the the parameters ε_i are chosen to be $\varepsilon_i = \pm 1$ with $\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4 = 1$. There are 8 choices of signs ε_i and 8 choices for the leading vertex i.e. the vertex where $1 + i$ occurs. One can check that this configuration is a SIC by computing all the hermitian products. One has only to perform 4 calculations depending on the distance between the corresponding leading vertices.



8.4 The Heisenberg group

Except for the Hoggar SIC all the known SIC are related to a finite Heisenberg group.

Heisenberg SIC The projective unitary group $\mathrm{PU}(d)$ which is the quotient of the unitary group $\mathrm{U}(d)$ by its center $\mathbb{S}^1$ acts on the set $\mathbb{P}(\mathbb{C}^d)$ of lines of $\mathbb{C}^d$. All the known SICs are orbits of a finite abelian group A of order d^2 of the projective unitary group $\mathrm{PU}(d)$. In all known cases, except in the case of the Hoggar SIC for which $A = (\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/2\mathbb{Z})^3$, the group is a product $A = (\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/d\mathbb{Z})$. In all these cases the group A is a quotient of a subgroup H_d of $\mathrm{U}(d)$ called a Heisenberg or Heisenberg group.

Definition 8.9. *The Heisenberg group H_d is the subgroup of $U(d)$ generated by the matrices*

$$E = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } F = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta_d & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \zeta_d^{d-1} \end{pmatrix} \text{ where } \zeta_d = e^{2i\pi/d}.$$

The projective Heisenberg group PH_d is the image of the Heisenberg group in the projective unitary group $PU(d)$

Lemma 8.10. *The center Z_d of H_d is a cyclic group of order d generated by $\zeta_d \mathbf{1}_d$, the group PH_d is isomorphic to $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$, and there is an exact sequence*

$$1 \longrightarrow Z_d \longrightarrow H_d \longrightarrow PH_d \longrightarrow 1.$$

Proof. This follows from the equality $FE = \zeta_d EF$ which says that the two matrices E, F commute modulo the center. □

We note that the group PH_d acts in the projective space $\mathbb{P}(\mathbb{C}^d)$. It also acts by conjugation on the set of rank one projectors of $\mathbb{C}^d$.

Definition 8.11. *A HSIC is a SIC which is an orbit under the Heisenberg group H_d. A line $\mathbb{C}v_0$ or a projector P_0 in such an orbit is called a fiducial line or a fiducial projector, and the vector v_0 is called a fiducial vector.*

Conjecture 8.12. *For all $d \geqslant 2$, there exists a HSIC in $\mathbb{C}^d$.*

This conjecture has been checked up to $d = 180$.

Remark 8.13. The Hoggar SIC we have seen in section 8.3 is very much like a Heisenberg SIC in dimension 8, except that the cyclic group $\mathbb{Z}/8\mathbb{Z}$ has been replaced by another abelian group $(\mathbb{Z}/2\mathbb{Z})^3$ of order 8. It is not known whether other finite abelian groups can give rise to SICs by a similar construction.

Conjecture 8.14. *For all $d \geqslant 2$, all the SICs of $\mathbb{C}^d$ are orbits of an abelian subgroup of $PU(d)$ of order d^2.*

It is possible that all SICs are HSIC, except for the Hoggar SIC, eventhough this might look too optimistic.

8.5 Equations defining the fiducial projectors

We describe now the explicit equations that define a fiducial projector.

We think of a projector P_0 in $\mathbb{C}^d$ as a line $[v_0] = [z_0, \dots, z_{d-1}] \in \mathbb{P}(\mathbb{C}^d)$ and an hyperplane $[f_0] = [w_0, \dots, w_{d-1}] \in \mathbb{P}(\mathbb{C}^{d*})$ with $f_0(v_0) \neq 0$ that is $\sum\limits_k z_k\, w_k \neq 0$. The projector is given by $P_0(v) = \frac{f_0(v)}{f_0(v_0)} v_0$. We think of the indices as elements of $\mathbb{Z}/d\mathbb{Z}$.

Proposition 8.15. *a) The projector P_0 is hermitian if and only if $[f_0] = [\overline{v_0}]$.*
b) The projector P_0 is fiducial if and only if for all $\ell \neq 0$, $m \neq 0$ one has

$$\sum_k z_k\, w_{k+\ell}\, w_{k+m}\, z_{k+\ell+m} \;=\; 0 \quad (E_{\ell,m}) \qquad \text{and} \tag{8.3}$$

$$\sum_k z_k\, w_k\, w_{k+\ell}\, z_{k+\ell} \quad \text{does not depend on } \ell \neq 0. \tag{8.4}$$

Proof. The projector P_0 is fiducial if and only if the function

$$(m,n) \mapsto Tr(P_0 P_{m,n}) \;\text{ is constant outside } 0,$$

where $P_{m,n} := E^m F^n P_0 F^{-n} E^{-m}$. We compute, with $\ell = h - k$,

$$\begin{aligned} Tr(P_0 P_{m,n}) &= f_0(E^m F^n v_0) f_0(F^{-n} E^{-m} v_0) \\ &= (\sum_k z_k w_{k+m} \zeta_d^{nk})(\sum_h w_h z_{h+m} \zeta_d^{-nh}) \\ &= \sum_\ell f_m(\ell) \zeta^{-\ell n} \end{aligned}$$

where $f_m(\ell) := \sum\limits_k z_k\, w_{k+\ell}\, w_{k+m}\, z_{k+\ell+m}$.

When $m \neq 0$ the Fourier transform of the function f_m is constant, therefore the function f_m is zero outside 0. This gives (8.3).

When $m = 0$ the Fourier transform of the function f_0 is constant outside 0, therefore the function f_0 is also constant outside 0. This gives (8.4). □

Remark 8.16. The system of equations (8.3) and (8.4) is overdetermined: there are $d^2 - d - 1$ equations, it is surprising that it always admits solutions in $\mathbb{P}(\mathbb{C}^d) \times \mathbb{P}(\mathbb{C}^d)$.

8.6 Other examples of SIC

SIC in dimension 4
The first non trivial HSICs were discovered in dimension 4, 5 and 6 by Zauner in 1999 in his PhD thesis which appeared in [47]. Here is his 4 dimensional example.

Lemma 8.17. *For $d = 4$, a fiducial vector for a HSIC is given by*

$$v_{00} = (x{+}u, u{-}i, x{-}u, u{+}i)$$

where $u := (1 + i)/\sqrt{2} = e^{i\pi/4}$ *and* $x := \sqrt{\sqrt{5} + 2}$.

In the basis f_1, f_2, f_3, f_4, where

$$f_1 = (1, 0, 1, 0),\ f_2 = (u, 0, -u, 0),\ f_3 = (0, u, 0, u),\ f_4 = (0, -i, 0, i)$$

the vector v_{00} becomes $v'_{00} = (x, 1, 1, 1)$ and the matrices E and F read as

$$E' = u\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix} \text{ and } F' = u\begin{pmatrix} 0 & 1 & 0 & 0 \\ -i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

One notice that $E'^2 = \mathrm{diag}(1, -1, 1, -1)$ and $F'^2 = \mathrm{diag}(1, 1, -1, -1)$ and that one can forget the scalar factor u to describe the SIC. In this basis, the SIC is formed by the 16 lines generated by the following 16 column vectors :

$$\begin{array}{cccccccccccccccc} x & x & x & x & i & -i & i & -i & i & -i & i & -i & i & -i & i & -i \\ 1 & 1 & -1 & -1 & x & x & x & x & -i & i & i & -i & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & x & x & x & x & -i & i & i & -i \\ 1 & -1 & -1 & 1 & -i & i & i & -i & 1 & 1 & -1 & -1 & x & x & x & x \end{array}$$

Indeed, one can check that

$$\|v'_{00}\|^2 = \sqrt{5}\,|\langle v'_{00}, v'_{ij}\rangle|,$$

because $x^2{+}3 = \sqrt{5}(x^2{-}1) = \sqrt{5}\sqrt{2(x^2{+}1)}$.

SIC in dimension 7 **and** 19
Appleby discovered that in dimension 7, and also in dimension 19, there exist nice fiducial vectors v_0 whose coordinates z_k depend only on the quadratic

residue class of k mod d. This phenomenon does not seem to exist beyond these two dimensions $d = 7$ and 19. What is special in these two dimensions that gives rise to rather simple HSIC. This will be explained by the general conjectures that we will state in the following lectures.

Lemma 8.18. *For $d = 7$, there exists a HSIC in $\mathbb{C}^7 \simeq \mathbb{C}[\mathbb{F}_7]$ with fiducial vector $v_0 = \delta_0 + a\mathbf{1}_{\mathbb{F}_7^*} + ib\chi_0$ where χ_0 denotes the Legendre character, and where a and b are real numbers: $a = \frac{-1}{2\sqrt{2}}$ and $b = \frac{\sqrt{4\sqrt{2}-5}}{2\sqrt{2}}$.*

Proof. We have $v_0 = (1, z, z, w, z, w, w)$ with $z = a + ib$, $w = a - ib = \overline{z}$. Using indices in $\mathbb{Z}/7\mathbb{Z}$, we introduce the vector $c = (w, z, z^2, zw, zw, zw, w^2)$ with coordinates $c_m := z_m\overline{z_{m-1}}$ and $C_\ell = \sum_m c_m\overline{c_{\ell+m}}$, and one writes

$$\langle Ev_0 | F^k v_0\rangle = \sum_m c_m \zeta_7^{km} \text{ and } |\langle Ev_0 | F^k v_0\rangle|^2 = \sum_\ell C_\ell \zeta_7^{k\ell} \text{ for all } k. \qquad (8.5)$$

The equations that express that the vectors $E^j F^k v_0$ form a HSIC can be reduced to $C_\ell = 0$ for all $1 \leqslant \ell \leqslant 6$. This gives rise to only two equations where $s = z + w$ and $p = zw$,

$$\begin{aligned} C_2 = C_3 = C_4 = C_5 &= s^3 - (p + 2s - s^2)p = 0, \\ C_1 = C_6 &= s^4 - (3s^2 - s - 1)p = 0. \end{aligned}$$

Solving these equations give $s = \frac{-1}{\sqrt{2}}$ and $p = \frac{\sqrt{2}-1}{2}$.

We conclude by applying Proposition 8.15 and by checking that the vector v_0 we have just found satisfies Equations (8.3) and (8.4).

We have chosen v_0 so that the Equations $E_{\ell,m}$ of (8.3) for $\ell = 1$ and for m in $\mathbb{F}_7^*$ are satisfied. But the group $\mathbb{F}_7^*$ acting on the indices is a group of symmetries for these equations. Therefore, seen as equalities in the variables z and $w = \overline{z}$, Equation $E_{1,m}$ is the same as Equation $E_{\ell,\ell m}$ for all $\ell \neq 0$. This proves that Equations (8.3) are satisfied. For the same reason, Equations (8.4) are satisfied for all z. □

The following lemma tells us that a similar calculation works with $d = 19$.

Lemma 8.19. *For $d = 19$, there exists a HSIC in $\mathbb{C}^{19} \simeq \mathbb{C}[\mathbb{F}_{19}]$ with fiducial vector $v_0 = \delta_0 + a\mathbf{1}_{\mathbb{F}_{19}^*} + ib\chi_0$ where χ_0 denotes the Legendre character, and where a and b are real numbers: $a = \frac{\sqrt{5}-1}{2\sqrt{2}}$ and $b = \frac{\sqrt{5\sqrt{5}-7}}{4\sqrt{2}}$.*

Proof. The proof is similar but involves more calculations, we have

$$v_0 = (1, z, w, w, z, z, z, z, w, z, w, z, w, w, w, w, z, z, w)$$

with $z = a + ib$ and $w = a - ib = \overline{z}$. Using indices in $\mathbb{Z}/19\mathbb{Z}$, the vector c with coordinates $c_m := z_m\overline{z_{m-1}}$ is

$$c = (z, z, w^2, zw, z^2, zw, zw, zw, w^2, z^2, w^2, z^2, w^2, zw, zw, zw, z^2, zw, w^2).$$

Let $C_\ell = \sum_m c_m\overline{c_{\ell+m}}$. The equations (8.5) can be reduced to $C_\ell = 0$ for all $1 \leqslant \ell \leqslant 18$. Note that $C_\ell = C_{19-\ell}$ This gives rise to only three equations where $s = z + w$ and $p = zw$,

$$\begin{aligned} C_2 = C_7 = C_8 = C_9 &= 3p^2 - (s+2)sp + (s+1)s^3 = 0, \\ C_3 = C_4 = C_5 = C_6 &= -5p^2 + (s+2)sp + s^4 = 0, \\ C_1 &= (2s+1)s^3 - (4s^2 + 3s - 1)p = 0. \end{aligned}$$

Adding the first two equations, one gets

$$2p^2 = (2s+1)s^3 = (4s^2 + 3s - 1)p.$$

Plugging this value $2p = 4s^2 + 3s - 1$ in these equations gives
$4s^2 + 2s - 1 = 0$. This gives $s = \frac{\sqrt{5}-1}{4}$ and $p = \frac{\sqrt{5}-1}{8}$.
We conclude as for $d = 7$ that v_0 is indeed fiducial. □

In the following exercise, we construct a simular fiducial vector in dimension 7. The difference with Lemma 8.18, is that the new fiducial vector has real coordinates.

Exercise 8.20. We want to prove that, for $d = 7$, there also exists a HSIC in $\mathbb{C}^7 \simeq \mathbb{C}[\mathbb{F}_7]$ with fiducial vector $v_0 = \delta_0 + a\mathbf{1}_{\mathbb{F}_7^*} + b\chi_0$ where χ_0 denotes the Legendre character, and where a and b are real numbers: $a = \frac{-1-\sqrt{2}}{2}$ and $b = \frac{\sqrt{2\sqrt{2}-1}}{2}$. In other words $v_0 = (1, x, x, y, x, y, y)$ with $x = a + b$, $y = a - b$ real numbers. Using indices in $\mathbb{Z}/7\mathbb{Z}$, the vector c with coordinates $c_m := z_m\overline{z_{m-1}}$ is $c = (y, x, x^2, xy, xy, xy, y^2)$.
(a) Let $C_\ell = \sum_m c_m\overline{c}_{\ell+m}$. Check that the equations (8.5) van be reduced to $C_\ell = 0$ for all $1 \leqslant \ell \leqslant 6$.
(b) Check that these equations are, with $s = x + y$ and $p = xy$,

$$\begin{aligned} C_2 = C_3 = C_4 = C_5 &= (s^2 + 2s - p)p = 0, \\ C_1 = C_6 &= s^3 + (s^2 - 3s + 1)p = 0. \end{aligned}$$

(c) Solve these equations and get $s = -1 - \sqrt{2}$ and $p = 1$.
(d) Check as for $d = 7$ that this vector v_0 is fiducial.

Notes to Chapter 8.
Theorem 8.1 is due to Gerzon in 1970 and is quoted in [34, Thm 3.5]
Theorem 8.2 is due to Delsarte, Goethals and Seidel.
The starting point of this chapter is Zauner's PhD thesis [47].
The SIC in dimension 7 and 19 are due to Appleby in [3]

9 The metaplectic representation

In this lecture we first explain how the first non-trivial HSICs were found. We then explain the role of the metaplectic group and the importance of the Zauner matrix Z in the construction of HSICs.

Recall Recall that a SIC is a family of $n = d^2$ complex lines $D_1, \dots, D_n$ in $\mathbb{C}^d$ whose pairwise angles θ are the same. This angle is given by $\cos\theta = 1/\sqrt{d+1}$.

Recall that the Heisenberg group H_d is the subgroup of order d^3 of the unitary group U_d generated by the matrices

$$E = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } F = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta_d & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \zeta_d^{d-1} \end{pmatrix}. \tag{9.1}$$

where $\zeta_d = e^{2i\pi/d}$.

These two matrices commute modulo the center since $FE = \zeta_d EF$. The matrix E acts by translation on $\mathbb{C}[\mathbb{Z}/d\mathbb{Z}]$, while the matrix F acts by multiplication by a character of order d.

For all $d \geqslant 4$, one wants to find a fiducial vector v_0 of $\mathbb{C}^d$, that is a vector such that the lines generated by the images $E^jF^kv_0$ form a SIC. Such a SIC is called a HSIC.

9.1 The gradient flow

Proposition 9.1. *Let v be a unitary vector in $\mathbb{C}^d$.*
(a) One has the equality $\sum_{jk\neq 00} |\langle v|E^jF^kv\rangle|^2 = d-1$.
(b) One also has the inequality $\mathcal{E}(v) := \sum_{jk\neq 00} |\langle v|E^jF^kv\rangle|^4 \geqslant \dfrac{d-1}{d+1}$.
(c) This inequality is an equality if and only if v is fiducial.

Exercise 9.2. (Schur lemma) Let $\rho : G \to \mathrm{GL}(d,\mathbb{C})$ be an irreducible finite dimensional representation of a group G. Let $A \in \mathcal{M}(d,\mathbb{C})$ be a matrix that commutes with G, i.e. such that $\rho(g)A = A\rho(g)$ for all $g \in G$. Prove that A is a scalar matrix.
Indication: Note that the eigenspaces of A are G-invariant.

Proof of Proposition 9.1. (*a*) The operator

$$A_v := \textstyle\sum_{h\in H_d} |hv\rangle\langle hv| \in \mathcal{M}(d,\mathbb{C})$$

commutes with H_d. Hence, by Schur lemma, one has $A_v = \lambda\mathbf{1}$ for some scalar λ. Comparing the traces, one gets $\lambda = |H_d|/d = d^2$. Therefore, one has

$$\textstyle\sum_{jk\neq 00} |\langle v|E^jF^kv\rangle|^2 \;=\; \frac{1}{d}\langle v|A_vv\rangle - 1 \;=\; d-1.$$

(*b*) By Cauchy Schwartz inequality, one has

$$\textstyle\sum_{jk\neq 00} |\langle v|E^jF^kv\rangle|^4 \;\geqslant\; \frac{1}{d^2-1}\sum_{jk\neq 00} |\langle v|E^jF^kv\rangle|^2 \;=\; \frac{(d-1)^2}{d^2-1} \;=\; \frac{d-1}{d+1}.$$

(*c*) In case of equality all the $|\langle v|E^jF^kv\rangle|$ are equal and v is fiducial. □

9.2 Experimental datas

The first non trivial HSICs were found thanks to a computer program who was looking for a minimum of this quantity $\mathcal{E}(v)$ called the energy, by following the gradient flow. The main difficulty when the dimension d increases is that this energy has a lot of minimas. As soon as one is near a minimum of the energy, the speed of convergence is very fast, and one can easily obtain the fiducial vector with a precision of a few hundred digits. Unfortunately there are also a lot of critical values slowing down the speed of convergence of the algorithm. Worse there are also many local minima that are not fiducial vectors and that trap the gradient flow. Their number also increases quickly with the dimension.

Another more efficient algorithm to find HSICs relies on solving the overdetermined polynomial system (8.3-8.4) by the Newton method. This gives a list of fiducial vectors. The following experimental output seems to indicate that this question is out of reach by an elementary approach.

For $d = 4$, there are 256 fiducial vectors that correspond to 16 SICs.
For $d = 5$, there are 2000 fiducial vectors that correspond to 80 SICs.
For $d = 11$, there are 319440 fiducial vectors that correspond to 2640 SICs.

As we can see, the number of HSIC grows quickly with d. This is mainly due to the presence of a large normalizer PN_d of the projective Heisenberg group $PH_d = (\mathbb{Z}/d\mathbb{Z})^2$ in the projective unitary group PU_d. In dimension

4, 5, 6 all the HSIC seem to be unitarily conjugate by an element of the projective normalizer. This seems to be the case for only finitely many values of d.

9.3 The normalizer of the Heisenberg group

We describe now the normalizer of H_d in $U(d)$ which acts on the HSICs.

Let N_d be the normalizer of the Heisenberg group H_d in $U(d)$. Let PH_d be the image of H_d in $PU(d)$, and let PN_d be the image of N_d in $PU(d)$.

Proposition 9.3. *The action by conjugation of PN_d on $PH_d \simeq (\mathbb{Z}/d\mathbb{Z})^2$ gives an exact sequence*

$$1 \longrightarrow (\mathbb{Z}/d\mathbb{Z})^2 \longrightarrow PN_d \xrightarrow{\varphi_0} SL(2,\mathbb{Z}/d\mathbb{Z}) \longrightarrow 1. \tag{9.2}$$

Example 1 Let $x := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. The element x mod d is the image $\varphi_0(X)$ of the diagonal matrix of multiplication by the Gaussian function $X := (\eta_d^{j^2}\delta_{j,k})$, where $\eta_d := -e^{i\pi/d}$. Indeed, one computes

$$XEX^{-1} = \eta_d EF \quad\text{and}\quad XFX^{-1} = F\,. \tag{9.3}$$

Example 2 Let $s := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. The element s mod d is the image $\varphi_0(S)$ of the matrix of the Fourier transform $S := \frac{1}{\sqrt{d}}(\zeta^{jk})$. Indeed, one computes

$$SES^{-1} = F \quad\text{and}\quad SFS^{-1} = E^{-1}\,. \tag{9.4}$$

Exercise 9.4. Prove that the elements x and s generate the group $\mathrm{SL}(2,\mathbb{Z})$.

Exercise 9.5. Prove that the elements x mod d and s mod d generate the group $\mathrm{SL}(2,\mathbb{Z}/d\mathbb{Z})$.

Exercise 9.6. Prove that the representation of H_d in $\mathbb{C}^d$ given by the matrices E and F is irreducible.

Proof of Proposition 9.3. We first need to explain why the adjoint action $\varphi_0(U)$ of an element $U \in N_d$ belongs to $SL(2,\mathbb{Z}/d\mathbb{Z})$.

On the one hand, the matrices E, F satisfy the relation $FE = \zeta_d EF$. Hence their images $E' := UEU^{-1}$ and $F' = UFU^{-1}$ also satisfy the equality $F'E' = \zeta_d E'F'$.

On the other hand, since $\varphi_0(U)$ is an automorphism of the group $(\mathbb{Z}/d\mathbb{Z})^2$, it is given by the action of an integral matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. But the two matrices $E' = E^\alpha F^\gamma$ and $F' = E^\beta F^\delta$ satisfy the equality $F'E' = \zeta_d^{\alpha\beta-\beta\gamma} E'F'$. This proves that $\alpha\delta - \beta\gamma = 1$ and the matrix $\varphi_0(U)$ has determinant 1 in $\mathbb{Z}/d\mathbb{Z}$.

We now prove the surjectivity of the map φ_0. This follows from the two examples because $SL(2, \mathbb{Z}/d\mathbb{Z})$ is generated by x mod d and s mod d.

We finally describe the kernel of φ_0. Let U be an element of $U(d)$ that commute with E and F modulo scalars. One has

$$UEU^{-1} = \lambda E \text{ and } UFU^{-1} = \mu F,$$

where λ and μ belong to $\mathbb{C}^*$. In particular the eigenvalues of F and λF are the same. Hence there exists an integer j such that $\lambda = \zeta^j$. Since $E^j F E^{-j} = \zeta^{-j} F$, after replacing U by UE^j, we can assume that U commutes with F. Similarly, after replacing U by UF^k for a suitable integer k, we can also assume that U commutes with E. Then, by Schur lemma, U is a scalar matrix. This proves that the kernel of φ_0 is the group PH_d. □

Exercise 9.7. Prove that there exists only one irreducible unitary representation ρ of the Heisenberg group H_d for which the center acts by the faithful character: $\rho(\zeta\mathbf{1}) = \zeta\mathbf{1}$.
Indication: Study the action of $\rho(E)$ on the eigenspaces of $\rho(F)$.

Remark 9.8. Here is another point of view on Propositions 9.3. The group H_d has one and only one irreducible d-dimensional representation ρ, for each faithful character of the center of H_d. Hence, for all g in the group $\mathrm{Aut}_0(H_d)$ of automorphisms of H_d acting trivially on the center of H_d, the representations ρ and $\rho \circ g$ are equivalent and there exists a unitary matrix u_g such that $\rho \circ g = u_g \rho(g) u_g^{-1}$, for all g in H_d. This projective representation of $\mathrm{Aut}_0(H_d)$ is called the metaplectic representation or, sometimes also, the "symplectic spinor" representation.

9.4 Displacement operators

We want to lift the elements of PH_d as elements of $U(d)$. We can not require that these lifts commute, but we will choose these lifts in a very precise way which is invariant by conjugacy by elements of PN_d. When d is odd, we will be able to do it in a one-to-one way and to parametrize the lifts with the plane $(\mathbb{Z}/d\mathbb{Z})^2$. When d is even, the lifts will not be one-to-one and will be parametrized by $(\mathbb{Z}/2d\mathbb{Z})^2$.

Definition 9.9. *We set $d' = d$ for d odd, and $d' = 2d$ for d even.*
For $p = (j,k)$ in the "plane" $(\mathbb{Z}/d'\mathbb{Z})^2$, we set

$$D_p = \eta_d^{jk} E^j F^k = \eta_d^{-jk} F^k E^j \text{ where } \eta_d = -e^{i\pi/d}. \tag{9.5}$$

Remember that $\eta_d^2 = \zeta_d$ and that $\eta_d^d = (-1)^{d-1}$. The operators D_p are called displacement operators. They are well defined because, for $p \in \mathbb{Z}^2$,

$$\begin{cases} D_{p+dq} = D_p & \text{when } d \text{ is odd,} \\ D_{p+2dq} = D_p & \text{when } d \text{ is even.} \end{cases} \tag{9.6}$$

Note that these operators D_p live in the group $H'_d := H_d \cup \eta_d H_d$ which is equal to H_d when d is odd.

Remark 9.10. The choice of normalization might look strange at first glance. For the reader familiar with Lie groups, a way to "undertand" this formula, is to think of it as an analog of the exponential map. Indeed, in the real Heisenberg group

$$H_{\mathbb{R}} = \{m_{j,k,\ell} := \exp \begin{pmatrix} 0 & k & \ell \\ 0 & 0 & j \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & k & \ell + \frac{jk}{2} \\ 0 & 1 & j \\ 0 & 0 & 1 \end{pmatrix} \mid (j,k,\ell) \in \mathbb{R}\}$$

the analog of (9.5) is the equality

$$m_{j,k,0} \;=\; m_{0,0,\frac{jk}{2}}\, m_{0,j,0}\, m_{0,0,k} \;=\; m_{0,0,\frac{-jk}{2}}\, m_{0,0,k}\, m_{0,j,0}.$$

Remark 9.11. The choice of this normalization for the displacement operator will be crucial when we will study the Galois group action on the phases $\langle v_0 | D_p v_0 \rangle$ of a HSIC associated to a fiducial vector v_0 of norm 1.

This notation is convenient as one can see in the following two lemmas.

Lemma 9.12. *One has the equalities, for all p, q in $(\mathbb{Z}/d'\mathbb{Z})^2$*

$$\begin{cases} D_p^* &=& D_p^{-1} \;=\; D_{-p}, \\ D_p D_q &=& \eta_d^{p_2 q_1 - p_1 q_2} D_{p+q}, \\ D_{p+dq} &=& (-1)^{p_2 q_1 - p_1 q_2} D_p \quad \text{for } d \text{ even} \\ D_{(1+d)p} &=& D_p. \end{cases} \tag{9.7}$$

Remark 9.13. In particular, the last equation says that, when d is even, given p in $(\mathbb{Z}/2d\mathbb{Z})^2$, the four displacement operator D_{p+dq} are equal up to sign.

Proof of Lemma 9.12. One computes

$$D_p^* = D_p^{-1} = \eta_d^{-p_1p_2} F^{-p_2} E^{-p_1} = \eta_d^{p_1p_2} E^{-p_1} F^{-p_2} = D_{-p}.$$

Similarly, one computes,

$$D_pD_q \;=\; \eta_d^{p_1q_1+p_2q_2+2p_2q_1} E^{p_1} E^{q_1} F^{q_1} F^{q_2} \;=\; \eta_d^{p_2q_1-p_1q_2} D_{p+q}.$$

The last equations follow since $D_{dq} = \mathbf{1}$ for all q. □

9.5 The projective metaplectic group

We would like to find a section for the projection φ_0 in (9.2). We will see that this is the case when d is odd. We will also see that for d even this is not the case, and that we have to introduce the group $\mathrm{SL}(2,\mathbb{Z}/2d\mathbb{Z})$

Remark 9.14. The reader should first focus on the easier case where d is even, in order to avoid the subtleties and technicalities needed for the case where d is odd. We will see in the next lectures that these subtleties will have a strong influence on the field of definitions of HSIC. One crucial difference between the case d even and d odd is that the matrix X in (9.3) satisfies

$$\begin{aligned} X^d &= \mathbf{1} \text{ when } d \text{ is odd} \\ &= ((-1)^j\delta_{j,k}) \text{ when } d \text{ is even} \end{aligned}$$

We first define the projective metaplectic group by using the displacement operator D_p defined in (9.5).

Definition 9.15. *Let $d \geqslant 2$. Set $d' = d$ for d odd and $d' = 2d$ for d even. The projective metaplectic group is the group*

$$\begin{aligned} PM_d \;=\; \{U \in PN_d \mid & \text{ there exists } g = \varphi(U) \in \mathrm{SL}(2,\mathbb{Z}/d'\mathbb{Z}) \\ & \text{such that } UD_pU^{-1} = D_{gp} \text{ for all } p \in (\mathbb{Z}/d'\mathbb{Z})^2\} \end{aligned} \tag{9.8}$$

Note that the element UD_pU^{-1} is well defined as an element of $U(d)$, and that we require Equality (9.8) to hold in $U(d)$.

We have to introduce the matrix

$$\mathbf{1}' = \begin{pmatrix} 1+d & 0 \\ 0 & 1+d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}/d'\mathbb{Z}),$$

because, by Lemma 9.12, one has

$$D_{\mathbf{1}'p} = D_p \text{ for all } p \in (\mathbb{Z}/d'\mathbb{Z})^2$$

This matrix $\mathbf{1}'$ is the identity when d is odd and has order 2 when d is even.

We denote by $\mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})/\mathbf{1}'$ the quotient of the group $\mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$ by the subgroup generated by $\mathbf{1}'$.

Remark 9.16. Note that when d is even one has an exact sequence

$$1 \longrightarrow K_d \longrightarrow \mathrm{SL}(2, \mathbb{Z}/2d\mathbb{Z}) \xrightarrow{\pi} \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z}) \longrightarrow 1 \tag{9.9}$$

where

$$K_d = \{g = \begin{pmatrix} 1+rd & sd \\ td & 1+rd \end{pmatrix} \mid (r, s, t) \in (\mathbb{Z}/2\mathbb{Z})^3\}$$

is a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$.

Proposition 9.17. (a) *The map* $\varphi : PM_d \to \mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})/\mathbf{1}'$ *is uniquely defined and is a group morphism.*
(b) *The group* PM_d *is the subgroup of* PN_d *generated by* X *and* S.
(c) *The morphism* $\varphi : PM_d \to \mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})/\mathbf{1}'$ *is an isomorphism.*
($d1$) *Assume* d *is odd. Then one has* $PM_d \cap PH_d = \{\mathbf{1}\}$ *and the morphism* $\varphi_0 : PM_d \to \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$ *is an isomorphism. In particular the group* PN_d *is a semidirect product*

$$PN_d = PM_d \ltimes PH_d \simeq \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z}) \ltimes (\mathbb{Z}/d\mathbb{Z})^2.$$

($d2$) *Assume* d *is even. Then the intersection* $PM_d \cap PH_d$ *is the group* $K'_d := \{D_{qd/2} \mid q \in (\mathbb{Z}/2\mathbb{Z})^2\}$ *which is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^2$. *In particular, one has an exact sequence*

$$1 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow PM_d \xrightarrow{\varphi_0} \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z}) \longrightarrow 1$$

Proof. (a) When d is odd, the map $p \mapsto D_p$ is injective hence g is unique and φ is well defined. When d is even, for all p, p' in $(\mathbb{Z}/2d\mathbb{Z})^2$, the equality $D_p = D_{p'}$ implies that $p' \equiv p \bmod d$ and, writing $p' = p + dq$ with $q \in (\mathbb{Z}/2\mathbb{Z})^2$, that one has $p_1 q_2 \equiv p_2 q_1 \bmod 2$. This proves that g is unique modulo the subgroup $\{\mathbf{1}, \mathbf{1}'\}$ and φ is well defined.

(b) and (c) We first check that X and S belong to PM_d. We compute in $U(d)$, for $p = (p_1, p_2) \in (\mathbb{Z}/d'\mathbb{Z})^2$, using (9.3) and (9.4),

$$\begin{aligned} XD_pX^{-1} &= \eta_d^{p_1p_2} XE^{p_1}F^{p_2}X^{-1} = \eta_d^{p_1p_2}\eta_d^{p_1}(EF)^{p_1}F^{p_2} \\ &= \eta_d^{p_1p_2}\eta_d^{p_1^2}E^{p_1}F^{p_1+p_2} = D_{xp}, \end{aligned}$$

$$\begin{aligned} SD_pS^{-1} &= \eta_d^{p_1p_2} SE^{p_1}F^{p_2}S^{-1} = \eta_d^{p_1p_2}F^{p_1}E^{-p_2} \\ &= \eta_d^{-p_1p_2}E^{-p_2}F^{p_1} = D_{sp}. \end{aligned}$$

This proves (9.8).

We now prove the injectivity of φ. If an element $U \in PN_d$ is in the kernel of φ, it commutes with all the matrices D_p. Hence it comutes with the Heisenberg group, and by Schur lemma it is trivial in $PU(d)$.

Finally the surjectivity of φ and the fact that X and S generate PM_d follow from the fact that x mod d' and s mod d' generate $\mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$ and from the injectivity of φ.

(d) We note that one has the equalities in $U(d)$, for $p \in (\mathbb{Z}/d'\mathbb{Z})^2$

$$D_pD_qD_p^{-1} = \zeta_d^{p_2q_1-p_1q_2}D_q. \qquad (9.10)$$

($d1$) When d is odd Equation (9.10) tells us that $PM_d \cap PH_d = \{\mathbf{1}\}$. Therefore the map φ is nothing but the map φ_0 in Proposition 9.3.

($d2$) When d is even Equation (9.10) tells us that $PM_d \cap PH_d = K'_d$. Therefore, the kernel of φ_0 is the group K'_d.

Note that one has the equality $\varphi_0 = \pi \circ \varphi$ on PM_d. □

Assume d is odd, we have defined the projective metaplectic group $PM_d \simeq \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$ as a subgroup of $PU(d)$. The following corollary tells us that this group lifts as a subgroup M_d of $U(d)$. This is the metaplectic group introduced by Weil. In this case the metaplectic group M_d is isomorphic to $\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$. This is the content of the following corollary.

Corollary 9.18. *Assume d is odd.*
(a) *Then there exists a morphism*

$$\psi : \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z}) \to U(d) \text{ such that} \qquad (9.11)$$

$$\psi(g)D_p\psi(g)^{-1} = D_{gp}, \text{ for all } p \in (\mathbb{Z}/d\mathbb{Z})^2. \qquad (9.12)$$

The group $M_d := \psi(\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z}))$ is called the metaplectic group.
(b) *The group M_d is generated by X and $i^{(1-d)/2}S$.*

Proof. The main remark is that the projective metaplectic representation of the group $PM_d \simeq \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$ in the vector space $V = \mathbb{C}^d$ is not irreducible, but decomposes as a sum $V = V^+ \oplus V^-$ of invariant subspaces, where V^+

and V^- are respectively the subspaces of even and odd functions on $\mathbb{Z}/d\mathbb{Z}$, and that

$$\dim V^+ - \dim V^- = 1. \tag{9.13}$$

(a) For every g in $\mathrm{SL}(2,\mathbb{Z}/d\mathbb{Z})$ we choose an element $\psi(g) \in U(d)$ such that

$$\varphi_0(\psi(g)) = g \text{ and } \det_{V^+}(\psi(g)) = \det_{V^-}(\psi(g)).$$

By (9.13), this element $\psi(g)$ exists and is unique. Therefore, for all g, g' in $\mathrm{SL}(2,\mathbb{Z}/d\mathbb{Z})$ we must have $\psi(gg') = \psi(g)\psi(g')$. And ψ is a group morphism.

(b) The matrix X, which is the multiplication by a gaussian function, belongs to M_d because

$$\det_{V^+}(X) = \det_{V^-}(X).$$

The matrix S of the Fourier transform satisfies $S^2 = \mathbf{1}$ on V^+. Hence its multiple λS that belongs to M_d can be determined by the formula

$$\lambda = \det_{V^-}(S)/\det_{V^+}(S) = \det_V(S) = i^{(1-d)/2}.$$

The last equality computing the determinant of the Fourier transform follows from the list of eigenvalues of S given in Proposition 1.6. □

Remark 9.19. When d is prime to 3 the morphism ψ is unique and the metaplectic group is uniquely defined. This follows from the fact that when d is prime to 6, the group $\mathrm{SL}(2,\mathbb{Z}/d\mathbb{Z})$ is perfect.

Remark 9.20. The name *Clifford group* is often used in the SIC-POVM litterature, as in [28], for the normalizer PN_d of PH_d in $U(d)$. In group theory one uses the name *metaplectic group* for the cover of the symplectic group that normalizes the Heisenberg group H in the unitary group $U(\mathcal{H})$ of the *Stone-von Neumann* irreducible unitary representation $\mathcal{H}$ of H. The corresponding projective unitary representation of the symplectic group in $\mathcal{H}$ is called *the Weil representation* or *the metaplectic representation.*

9.6 The Zauner matrix

We now come back to HSICs. In the conjectural description of the HSICs there is an important symmetry of order 3 discovered by Zauner, that lives in the metaplectic group.

We denote by $z \in \mathrm{SL}(2,\mathbb{Z})$ the element of order 3 $z := xs = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. It correspond to the matrix XS. The Zauner matrix Z is a suitable normalization of XS thanks to a 24th root of unity $\zeta_{24} = e^{i\pi/12}$. This normalisation of Z will be useful in Conjecture 9.23 and in the following lemma.

Lemma 9.21. *The Zauner matrix* $Z := \frac{\zeta_{24}^{d-1}}{\sqrt{d}}(\eta_d^{j(j+2k)})$ *has order* 3.

Up to scalar, the Zauner matrix Z is the unique unitary transformation $Z \in U_d$ such that

$$ZEZ^{-1} = F \text{ et } ZFZ^{-1} = \tau E^{-1}F^{-1}.$$

Proof of Lemma 9.21. We recall Gauss formula given in Lemma 1.7,

$$\frac{1}{\sqrt{d}} \sum_{1 \leqslant k \leqslant d} \eta_d^{k^2} = \zeta_8^{1-d} \text{ where } \zeta_8 = e^{i\pi/4} = \zeta_{24}^3.$$

One computes using Gauss formula an entry of the square matrix,

$$\begin{aligned} (Z^2)_{j\ell} &= \frac{\zeta_{24}^{2d-2}}{d} \sum_{1 \leqslant k \leqslant d} \eta_d^{j^2} \eta_d^{2jk} \eta_d^{k^2} \eta_d^{2k\ell} \\ &= \frac{\zeta_{24}^{2d-2}}{d} \eta_d^{-\ell^2} \eta_d^{-2j\ell} \sum_{1 \leqslant m \leqslant d} \eta_d^{m^2} \quad \text{where } m = j+k+\ell, \\ &= \frac{\zeta_{24}^{1-d}}{\sqrt{d}} \eta_d^{-\ell(\ell+2j)} \;=\; \overline{Z}_{\ell j}. \end{aligned}$$

This proves that $Z^2 = Z^*$ and, since Z is unitary, that $Z^3 = ZZ^* = \mathbf{1}$. □

One can deduce the list of eigenvalues of Z counted with multiplicity, as in Proposition 1.6 for the Fourier transform.

Proposition 9.22. *Let* $d \geqslant 2$. *The eigenvalues of the Zauner matrix* Z *on* $\mathbb{Z}/d\mathbb{Z}$ *are given by the first* d *elements of the list:* $1, \zeta_3, 1, \zeta_3^2, \zeta_3, 1, \zeta_3^2, \zeta_3, 1 \ldots$

Proof. We only need to check that for $0 \leqslant \ell \leqslant 2$ the trace of the ℓ^{th}-power of the Zauner matrix $tr(Z^\ell)$ is equal to the sum of the ℓ^{th}-power of this sequence.

Since $tr(Z^0) = d$ and $tr(Z^2) = \overline{tr(Z)}$, this means that one has to check

$$tr(Z) = \begin{cases} 1 & \text{for } d \equiv 1 \bmod 3, \\ \zeta_6 & \text{for } d \equiv 2 \bmod 3, \\ \sqrt{3}\,\zeta_{12} & \text{for } d \equiv 0 \bmod 3. \end{cases} \tag{9.14}$$

We use Formula (1.7) with $c = 3$, This gives

$$\begin{aligned} tr(Z) &= \zeta_{24}^{d-1} \tfrac{1}{\sqrt{d}} \sum_k \eta_d^{3k^2} = \zeta_{24}^{d-1}\, \zeta_8^{1-3d}\, \tfrac{1+2\zeta_3^d}{\sqrt{3}} \\ tr(Z) &= \zeta_{12}^{1-4d}\, \tfrac{1+2\zeta_3^d}{\sqrt{3}}. \end{aligned}$$

Distinguishing the three values for d mod 3, one gets (9.14). □

The choice of normalization for the Zauner matrix is useful to point out a suitable eigenspace of Z in which we will look for a fiducial vector. Based on his experimental datas, Zauner conjectured:

Conjecture 9.23. *For all $d \geqslant 2$, there exists a Z-invariant fiducial vector, i.e. a fiducial vector v_0 such that $Zv_0 = v_0$.*

The algorithm that looks for a fiducial line that is Z-invariant is much faster because we are looking for a solution in a projective subspace of dimension $[\frac{d}{3}]$. For instance, for $d = 4$ or 5 we are looking for solutions of polynomial equations in 1 variable.

Appleby has noticed, that sometimes there are also fiducial vectors in other eigenspaces of the Zauner matrix.

Conjecture 9.24.
When $d \equiv 1$ mod 3, there exists a fiducial vector v_0 such that $Zv_0 = \zeta_3^2 v_0$.
When $d \equiv 1$ mod 9, there exists a fiducial vector v_0 such that $Zv_0 = \zeta_3 v_0$.

9.7 Elements of order 3

Appleby has also conjectured a converse.

Conjecture 9.25. *The stabilizer of a HSIC in PN_d/PH_d always contain an element A of order 3.*

In most of the cases, but not always, this stabilizer is generated by this element of order 3, and A is conjugate in PN_d to the Zauner matrix Z.

When $d \not\equiv 0$ mod 3, this element A always fixes a fiducial line.

The Zauner matrix Z comes from the element $z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ of order 3 of the group $\mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$. The following lemma tells us more on these elements of order 3.

Lemma 9.26. *Let $g \in SL(2, \mathbb{Z}/d\mathbb{Z})$ with d coprime to 3. Then one has the equivalence*
(a) g is conjugate to $z \iff tr(g) = -1$.
(b) If d is prime, all element g of order 3 is conjugate to z. Its centralizer C_g is a cyclic group $\begin{cases} \text{of order } d-1 \text{ if } d \equiv 1 \bmod 3, \\ \text{of order } d+1 \text{ if } d \equiv 2 \bmod 3. \end{cases}$

Exercise 9.27. Let $Q(x, y) = ax^2 + bxy + cy^2$ be a quadratic form on $(\mathbb{Z}/d\mathbb{Z})^2$. Assume that the discriminant $\Delta := b^2 - 4ac$ is invertible in $\mathbb{Z}/d\mathbb{Z}$. Prove that there exists $(x, y) \in (\mathbb{Z}/d\mathbb{Z})^2$ such that $Q(x, y) = 1$.
Indication: Deal successively with the following cases: First: d odd prime and use a basis where Q is diagonal. Second: $d = p^n$ odd prime power and lift a solution mod p^{n-1} to a solution mod p^n. Third: d power of 2 and deal first with $d = 2$, 4, 8 and lift again. Fourth: apply the chinese remainder theorem.

Proof of Lemma 9.26. (a) The implication $\Longrightarrow$ is clear. We prove $\Longleftarrow$. The inverse of the matrix $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is the matrix $g^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$. Therefore one has $g^{-1} + g = t\mathbf{1}$ where $t = \alpha + \delta$ is the trace. Since $t = -1$, one has $g^2 + g + \mathbf{1} = 0$. Choosing a basis of the form v, gv, one can see that g is conjugate to z in the group $\mathrm{GL}(2, \mathbb{Z}/d\mathbb{Z})$. We want more: we want this conjugacy to be in $\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$. We need to find a vector $v \in (\mathbb{Z}/d\mathbb{Z})^2$ such that $Q(v) := \det(v, gv) = 1$. The discriminant of this quadratic form Q is equal to $\Delta = (\delta - \alpha)^2 + 4\beta\gamma = -3$. Therefore it is invertible. Hence there exists v such that $Q(v) = 1$.

(b) Since $d = p \neq 3$ is prime, the ring $\mathbb{Z}/d\mathbb{Z}$ is the prime field $\mathbb{F}_p$ and g has two distinct eigenvalues $\omega^{\pm 1}$ in the field $\mathbb{F}_{p^2}$, which are primitive cube roots of unity and hence $tr(g) = -1$. Therefore, by Point (a), g is conjugate to z.

Finally, we recall that the multiplicative groups $\mathbb{F}_p^*$ and $\mathbb{F}_{p^2}^*$ are cyclic.

When $p \equiv 1 \bmod 3$, the eigenvalue ω belongs to $\mathbb{F}_p^*$, g is diagonalizable on $\mathbb{F}_p$ and the centralizer $C_g \simeq \mathbb{F}_p^*$ is a cyclic group of order $p - 1$.

When $p \equiv 2 \bmod 3$, the ring $\mathbb{F}_p[g]$ is isomorphic to the field $\mathbb{F}_{p^2}$ and the centralizer $C_g \simeq \{\lambda \in \mathbb{F}_{p^2}^* \mid \lambda^{p+1} = 1\}$ is a cyclic group of order $p + 1$. □

The following exercise tells us that Lemma 9.26.*b* is still valid for d a prime power, but not when d has two distinct prime divisors.

Exercise 9.28. Assume that $d = p^r$ is a prime power with $p \neq 3$.
(a) Prove that one has an exact sequence

$$1 \longrightarrow K \longrightarrow \mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z}) \longrightarrow \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z}) \longrightarrow 1 ,$$

where K is a normal p-subgroup.
(b) Prove that all element g of order 3 in $\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$ is conjugate to z.

Exercise 9.29. Assume $d = pq$ is the product of two primes not equal to 3.
(a) Prove that $\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z}) \simeq \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z}/q\mathbb{Z})$.
(b) Prove that there are 3 conjugacy classes of elements of order 3 in the group $\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$.

Notes to Chapter 9. Section 9.1 9.2 9.3 9.4

The description of the group of automorphisms of the Heisenberg group H_d is due to Appleby in [3].

The conjectures in this chapter and the previous one are an output of the works of Zauner in [47], Reves, Blume-Kohout, Scott and Caves in [37] and Appleby in [3].

In section 9.5 Proposition 9.17 is [3, Thm 1].

The explicit construction of the metaplectic representation over a finite field in Corollary 9.18 is due to Neuhauser in [36, Thm 4.3].

10 Fields of definition

In this lecture we state the first series of conjectures on the arithmetic of HSICs. To each fiducial projector P_0, we will associate a few number fields

$$\mathbb{Q} \subset \mathbb{K} \subset \mathbb{E}_0 \subset \mathbb{E}_1 \subset \mathbb{E}. \tag{10.1}$$

We will describe conjecturally striking properties of these number fields and of their Galois group. The constructions and Conjectures in this lecture are mainly due to Appleby, Yadsan-Appleby, Zauner in [4, Sec.7], to Appleby, Flammia, McConnel, Yard in [7] and to Kopp, Lagarias in [28] relying on numerical experiments due to Scott and Grassl in [39] and [38].

In the next lecture, we will describe explicitly the "unique" 5-dimensional HSIC. In this case we will see that

$$\mathbb{K} = \mathbb{E}_0 = \mathbb{Q}[\sqrt{3}]\ ,\ \ \mathbb{E}_1 = \mathbb{K}[iy_0] \text{ and } \ \mathbb{E} = \mathbb{E}_1[i],$$

where $y_0 = \sqrt{\frac{(1-c)\sqrt{3}+s}{24}}$, with $c = \cos(2\pi/5)$ and $s = \sin(2\pi/5)$. We will check directly that the extension $\mathbb{E}/\mathbb{K}$ is Galois with abelian Galois group. This is the first non trivial example that motivates the list of conjectures stated in this lecture.

A better conjectural description of these fields and their Galois action using the language of class field theory will be given in the following lectures.

10.1 Fiducial projectors

We first recall notation from previous lectures and add a few more. We assume $d \geqslant 4$. The projective Heisenberg group PH_d is the abelian subgroup of the projective unitary group $PU(d)$ of $\mathbb{C}^d$ which is generated by the two matrices $E = (\delta_{j,k+1})$ and $F = (\zeta_d^j \delta_{j,k})$, where $\zeta_d = e^{2i\pi/d}$. Let $\eta_d = -e^{i\pi/d}$.

We set $d' = d$ when d is odd and $d' = 2d$ when d is even, so that for $p = (p_1, p_2)$ in $(\mathbb{Z}/d'\mathbb{Z})^2$, the displacement operator $D_p = \eta_d^{p_1 p_2} E^{p_1} F^{p_2} \in \mathrm{U}(d)$ is well defined and satisfies (9.6) and (9.7).

The complex conjugation $\sigma_c \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ can be seen as an antiunitary involution of $\mathbb{C}^d$ or of $\mathbb{P}(\mathbb{C}^d)$. It sends HSIC to HSIC. We define the extended unitary group

$$\mathrm{EU}(d) = U(d) \cup U(d)\sigma_c \simeq (\mathbb{Z}/2\mathbb{Z}) \ltimes U(d),$$

and the projective extended unitary group $\mathrm{PEU}(d) = PU(d) \cup PU(d)\sigma_c$. We recall that N_d is the normalizer of H_d in $U(d)$, and PN_d is its normalizer in $\mathrm{PU}(d)$. Similarly we introduce the extended normalizer EN_d as the normalizer of H_d in $\mathrm{EU}(d)$ and the projective extended normalizer PEN_d as the normalizer of H_d in $\mathrm{PEU}(d)$. Both contain the complex conjugation σ_c.

Definition 10.1. *The field of definition of a subset S of $\mathcal{M}(d,\mathbb{C})$ or of $\mathbb{P}\mathcal{M}(d,\mathbb{C})$, is the smallest subfield $K \subset \mathbb{C}$ such that S is invariant by the group* $\mathrm{Gal}(\mathbb{C}/K)$.

When S is an algebraic subvariety, this means that S can be defined as the set of zeros of a family of polynomials with coefficients in K.

Lemma 10.2. (a) *The Heisenberg group H_d is defined over $\mathbb{Q}$.*
(b) *The normalizer PN_d is also defined over $\mathbb{Q}$.*

Proof. We check that these sets are invariant by the elements σ of the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. One has $\sigma(H_d) = H_d$. Indeed, there exists ℓ with $\ell \wedge d = 1$ such that $\sigma(\zeta_d) = \zeta_d^\ell$. Hence one has $\sigma(E) = E$ and $\sigma(F) = F^\ell$. □

We want to understand the set $\mathcal{F}_{d,h}$ of hermitian fiducial projectors.

$$\begin{aligned} \mathcal{F}_{d,h} &= \{P_0 \in \mathcal{F}_d \mid P_0^* = P_0\} \text{ where} \\ \mathcal{F}_d &= \{P_0 \in \mathcal{M}(d,\mathbb{C}) \mid P_0^2 = P_0, \ \ \mathrm{tr}(P_0) = 1 \ \text{ and} \\ & \qquad \mathrm{tr}(P_0 D_p P_0 D_{-p}) = \tfrac{1}{d+1} \ \text{ for all } p \text{ in } (\mathbb{Z}/d\mathbb{Z})^2\}. \end{aligned}$$

The set $\mathcal{F}_d$ of (non-necessarily hermitian) fiducial projectors is an algebraic subvariety of $\mathcal{M}(d,\mathbb{C})$.

The conjectures of the previous lectures can been extended to $\mathcal{F}_d$. Indeed, for $d \geqslant 4$, the set $\mathcal{F}_d$ is also conjectured by Waldron in [46, 14.27] to be a finite set. Its elements are then algebraic.

The defining equations of $\mathcal{F}_d$ seem at first glance to involve d^{th} roots of unity. A more careful look shows that one can get rid of these roots.

Lemma 10.3. *The set $\mathcal{F}_d$ is defined over $\mathbb{Q}$.*

Proof. This follows from the fact that H_d is defined over $\mathbb{Q}$. One can also apply Proposition 8.15. □

When $P_0 \in \mathcal{F}_{d,h}$ and $p \in (\mathbb{Z}/d\mathbb{Z})^2$ the projector $P_p := D_p P_0 D_{p^{-1}}$ is well defined, i.e. one has $P_{p+dq} = P_p$. The projectors P_p are also fiducial projectors. And the image of P_0 is a line in $\mathbb{C}^d$ whose H_d-orbit is a HSIC.

10.2 The real quadratic field of a HSIC

One of the first issue when one deals with the set $\mathcal{F}_{d,h}$ is that it is not defined over $\mathbb{Q}$ because, for $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, the image $\sigma(P_0)$ of a (hermitian) fiducial projector P_0 is a fiducial projector that is not necessarily hermitian. Let

$$\Delta_d := (d+1)(d-3) = (d-1)^2 - 4 \ \text{ and } \ \mathbb{K} := \mathbb{Q}[\sqrt{\Delta_d}].$$

The following conjecture predicts when this image is indeed hermitian.

Conjecture 10.4. *Let $\sigma \in Gal(\mathbb{C}/\mathbb{Q})$ and $P_0 \in \mathcal{F}_{d,h}$. Then, one has the equivalence:*

$$\sigma(P_0) \in \mathcal{F}_{d,h} \iff \sigma(\sqrt{\Delta_d}) = \sqrt{\Delta_d} \qquad (10.2)$$

Note that this condition does not depend on P_0. In particular, the field of definition of $\mathcal{F}_{d,h}$ is the field $\mathbb{K} := \mathbb{Q}[\sqrt{\Delta_d}]$.

Definition 10.5. *A geometric class is an orbit of* PEN_d *on $\mathcal{F}_{d,h}$.*
We denote by $[P_0]$ the geometric class of P_0.

Two fiducial projectors, or two fiducial lines or two HSICs, are said to be geometrically equivalent if they are in the same geometric class. Note that two fiducial lines in the same HSIC are always geometrically equivalent.

According to Conjecture 10.4 the group $\mathrm{Gal}(\mathbb{C}/\mathbb{K}) \ltimes \mathrm{PN}_d$ acts on $\mathcal{F}_{d,h}$. This group is the abstract semidirect product using the natural action of the group $\mathrm{Gal}(\mathbb{C}/\mathbb{K})$ by automorphisms on the group PN_d which is defined over $\mathbb{Q}$ by Lemma 10.2. This group contains PEN_d

Definition 10.6. *A multiplet is an orbit of* $\mathrm{Gal}(\mathbb{C}/\mathbb{K}) \ltimes \mathrm{PN}_d$ *on $\mathcal{F}_{d,h}$.*
We denote by $[[P_0]]$ the multiplet containing P_0.
The size of a multiplet is the number of geometric classes in it.

Note that Δ_d is the determinant of the quadratic equation

$$X^2 - (d-1)X + 1 \ = \ 0. \qquad (10.3)$$

For $d \geqslant 4$, the positive real root of this polynomial

$$\varepsilon_d := \tfrac{d-1+\sqrt{\Delta_d}}{2} \qquad (10.4)$$

is called the Zauner unit. It is a unit in the ring $\mathbb{Z}[\varepsilon_d]$. This ring is a subring of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of the real quadratic number field $\mathbb{K} = \mathbb{Q}[\varepsilon_d]$.

Definition 10.7. *We denote by D_0 the fundamental discriminant of $\mathbb{K}$. This means that $\Delta_d = f^2 D_0$ with f integer, $D_0 \neq 1$ and*
(i) either $D_0 \equiv 1 \bmod 4$ and D_0 square free,
(ii) or $D_0 = 4m^2$ with $m \equiv 2$ or $3 \bmod 4$ and m square free.

The positive fundamental discriminants are $D_0 = 5, 8, 12, 13, 17, 21, 24, \ldots$

Exercise 10.8. Write $\Delta_d = f^2 D_0$ with D_0 the fundamental discriminant of K. Let $\alpha_0 := \frac{D_0+\sqrt{D_0}}{2}$, so that $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha_0]$.
(a) Prove that the ring $\mathcal{O} := \mathbb{Z}[\varepsilon_d]$ is equal to $\mathbb{Z}[f\alpha_0]$.
$(b1)$ Find the list of integers $d = 4, 8, 19, 48, 124, \ldots$ for which $D_0 = 5$.
$(b2)$ Find the list of integers $d = 7, 35, 199, \ldots$ for which $D_0 = 8$.
$(b3)$ Find the list of integers $d = 5, 15, 53, 195, \ldots$ for which $D_0 = 12$.
This partially "explains" why it is easier to find HSICs in dimensions $d = 4, 5, 7, 8, 19$.

The integer f is called the conductor of the ring $\mathcal{O} = \mathbb{Z}[f\alpha_0]$.

Conjecture 10.9. *There is a natural bijection*

$$\{\text{multiplets in } \mathcal{F}_{d,h}\} \quad \longleftrightarrow \quad \{\text{divisors } f' \text{ of } f\}$$

Remark 10.10. We will understand better Conjecture 10.9, in the light of stronger conjectures that will follow. The divisor f' is the conductor of a unique intermediate ring $\mathcal{O}_f \subset \mathcal{O}_{f'} \subset \mathcal{O}_{\mathbb{K}}$. This ring $\mathcal{O}_{f'}$ will be related by class field theory to abelian extensions of $\mathbb{K}$, the ones that we introduce in the next section.

10.3 Fields of definition

We now introduce two fields $\mathbb{E}_0$ and $\mathbb{E}$ associated with a geometric class $[P_0]$ of a fiducial projector P_0.
⋆ The field $\mathbb{E}_0$ is the field of definition of the geometric class $[P_0]$.
⋆ The field $\mathbb{E}$ is $\mathbb{E} := \mathbb{L}[\eta_d]$ where $\mathbb{L}$ is the field of definition of P_0.

Lemma 10.11. *We assume Conjecture 10.4.*
(a) The fields $\mathbb{L}$ and $\mathbb{E}$ are invariant by complex conjugation σ_c, and one has the inclusion $\mathbb{E}_0 \subset \mathbb{R}$.
(b) The fields $\mathbb{E}_0$ and $\mathbb{E}$ depend only on the geometric class $[P_0]$.
(c) One has $\mathbb{K} \subset \mathbb{E}_0 \subset \mathbb{E}$.

Proof. (a) Since the projector P_0 is hermitian, the field $\mathbb{L}$ generated by the entries of P_0 is invariant by σ_c. Finally, since a PEN_d-orbit is always invariant by σ_c it is defined over $\mathbb{R}$ and one has $\mathbb{E}_0 \subset \mathbb{R}$.

($b1$) The field $\mathbb{E}_0$ depends only on $[P_0]$ by definition.

($b2$) Since all the elements U of the normalizer PN_d are defined over $\mathbb{Q}[\eta_d] \subset \mathbb{E}$, and since P_0 is defined over $\mathbb{E}$, all the elements UP_0U^{-1} of $[P_0]$ are also defined over $\mathbb{E}$. Hence the field $\mathbb{E}$ depends only on $[P_0]$.

($c1$) Since all the projectors in $[P_0]$ are defined over $\mathbb{E}$, one has $\mathbb{E}_0 \subset \mathbb{E}$.

($c2$) We will only use Conjecture 10.4 to prove the last inclusion $\mathbb{K} \subset \mathbb{E}_0$, if $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{E}_0)$ one has $\sigma(P_0) \in [P_0]$, hence one has $\sigma(\sqrt{\Delta_d}) = \sqrt{\Delta_d}$ and $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{K})$. This proves that $\mathbb{K} \subset \mathbb{E}_0$. □

Conjecture 10.12. (a) *The field* $\mathbb{E}$ *is a Galois extension of* $\mathbb{Q}$.
(b) *The field* $\mathbb{E}$ *is an abelian extension of* $\mathbb{K}$.

The group $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is a normal subgroup of index 2 in the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$. It contains the complex conjugation σ_c. Conjecture 10.12.b tells us that this subgroup is abelian.

Lemma 10.13. *We assume Conjectures 10.4 and 10.12.*
Then the subgroup $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ *is the centralizer* $C(\sigma_c)$ *of* σ_c *in* $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$

Proof. By Conjecture 10.12, the subgroup $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is abelian and hence is included in the centralizer $C(\sigma_c)$.

Conversely, if an element $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ commutes with σ_c, the projector $\sigma(P_0)$ is also hermitian and hence belong to $\mathcal{F}_{d,h}$. Hence, by Conjecture 10.4, one has $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{K})$. □

Remark 10.14. It may look at first glance surprising to have so many fields automorphisms σ that commute with σ_c, because the only non-trivial automorphism of $\mathbb{C}$ that commutes with σ_c is σ_c. The point is that the commutation of σ and σ_c is only required in the field $\mathbb{E}$.

Remark 10.15. According to Conjecture 10.12, the fields $\mathbb{E}_0$ and $\mathbb{E}$ depend only on the multiplet $[[P_0]]$.

Lemma 10.16. *We assume Conjectures 10.4 and 10.12.*
Then the degree $[\mathbb{E}_0 : \mathbb{K}]$ *is equal to the size of the multiplet* $[[P_0]]$.

Proof. The abelian group $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ sends geometric classes to geometric classes, and acts transitively on the set of geometric classes in $[[P_0]]$. By definition, the stabilizer of the geometric class $[P_0]$ is the subgroup $\mathrm{Gal}(\mathbb{E}_0/\mathbb{K})$.

Therefore the number of geometric classes in $[[P_0]]$ is the order of the quotient group $\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$ which is equal to $[\mathbb{E}_0 : \mathbb{K}]$. □

In the sequel of this lecture, we will state slightly more precise conjectures from the arithmetic point of view, and one will describe conjecturally the two Galois groups $\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$ and $\mathrm{Gal}(\mathbb{E}_0/\mathbb{K})$. A much more precise conjectural description of the fields $\mathbb{E}_0$ and $\mathbb{E}$ and of their Galois groups in terms of the idèles class group $C_{\mathbb{K}}$ will be given in the next lectures.

We recall that the ideal class group $\mathcal{C}l(\mathcal{O})$ of a finite index subring $\mathcal{O} \subset \mathcal{O}_{\mathbb{K}}$ is the group of invertible ideals modulo the principal ideals. When $\mathcal{O} = \mathcal{O}_{\mathbb{K}}$ all the ideals are invertible. In general the invertible ideals are those coprime to the conductor f.

Conjecture 10.17. *Let $P_0 \in \mathcal{F}_{d,h}$ and f' be the divisor of f associated to $[[P_0]]$. Then there is a group isomorphism* $\mathrm{Gal}(\mathbb{E}_0/\mathbb{K}) \simeq \mathcal{C}l(\mathcal{O}_{f'})$

We will see in a latter lecture that, in order to compute the ideal class group $\mathcal{C}l(\mathcal{O}_{f'})$, one can use the exact sequence

$$1 \longrightarrow \mathcal{O}_{\mathbb{K}}^*/\mathcal{O}_{f'}^* \longrightarrow \frac{(\mathcal{O}_{\mathbb{K}}/f'\mathcal{O}_{\mathbb{K}})^*}{(\mathbb{Z}/f'\mathbb{Z})^*} \xrightarrow{\pi} \mathcal{C}l(\mathcal{O}_{f'}) \longrightarrow \mathcal{C}l(\mathcal{O}_{\mathbb{K}}) \longrightarrow 1 \qquad (10.5)$$

This exact sequence tells us that the ideal class group $\mathcal{C}l(\mathcal{O}_f)$ is an extension of the classical ideal class group $\mathcal{C}l(\mathcal{O}_{\mathbb{K}})$ by an easily computable subgroup, the image of π. The quotient $\mathcal{C}l(\mathcal{O}_{\mathbb{K}})$ which is less easi to compute is often rather small.

Remark 10.18. Note that, conjecture 10.17 is uniform in $d \geqslant 4$, while the properties of the ring $\mathcal{O}_f = \mathbb{Z}[\varepsilon_d]$ and its class group heavily depend on d.

10.4 Galois action on correlations

We now introduce the field $\mathbb{E}_1$. We first define the subfield $\mathbb{E}_2 := \mathbb{E} \cap \mathbb{R}$. Let $\sigma_0 \in \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ such that $\sigma_0(\sqrt{\Delta_d}) = -\sqrt{\Delta_d}$. We define $\mathbb{E}_1 := \sigma_0(\mathbb{E}_2)$.

Since, by Conjecture 10.12, all the elements of $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ commute with the complex conjugation σ_c, the field $\mathbb{E}_1$ does not depend on the choice of σ_0. Moreover, this field $\mathbb{E}_1$ depends only on the multiplet $[[P_0]]$.

Lemma 10.19. *One has the inclusion $\mathbb{K}[\cos(2\pi/d')] \subset \mathbb{E}_1$.*

Proof. Indeed, the field $\mathbb{K}[\cos(2\pi/d')] = \mathbb{K}[\eta_d] \cap \mathbb{R}$ is a subfield of $\mathbb{E}_2$ which is Galois over $\mathbb{Q}$, hence it is invariant by σ_0 and it is included in $\mathbb{E}_1$. □

Let P_0 be a fiducial projector. It can be written as $P_0 = f_0 \otimes v_0$ with $f_0(v_0) = 1$ or $P_0 = |v_0\rangle\langle v_0|$.

Definition 10.20. *The correlations are the quantities*

$$u_p := f_0(D_p v_0) \ = \ \langle v_0 | D_p v_0 \rangle \ = \ \mathrm{tr}(P_0 D_p) \ , \ \text{ for } p \text{ in } (\mathbb{Z}/d'\mathbb{Z})^2.$$

By (9.6) and (9.7), they satisfy, for p, q in $(\mathbb{Z}/d'\mathbb{Z})^2$, $\ u_{-p} = \overline{u_p}$,

$$u_{p+dq} = u_p \quad \text{when } d \text{ is odd,} \tag{10.6}$$

$$u_{p+dq} = (-1)^{p_1q_2 - p_2q_1} u_p \ , \ \ u_{p+2dq} = u_{(1+d)p} = u_p \quad \text{when } d \text{ is even.} \tag{10.7}$$

The assumption that P_0 is fiducial can be written as

$$|u_p| = \tfrac{1}{\sqrt{d+1}} \ \text{ for all } p \not\equiv 0 \bmod d. \tag{10.8}$$

Lemma 10.21. *We assume Conjectures 10.4 and 10.12.*
Let $P_0 = |v_0\rangle\langle v_0|$ be a fiducial vector and $p \in (\mathbb{Z}/d'\mathbb{Z})^2$, $p \not\equiv 0$ mod d. Then for all $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{K})$ one also has

$$|\sigma(u_p)| = \tfrac{1}{\sqrt{d+1}} \ \text{ for all } p \not\equiv 0 \bmod d. \tag{10.9}$$

Proof. Since the extension $\mathbb{E}/\mathbb{K}$ is abelian, this element σ commutes with σ_c, and the projector $P_0' := \sigma(P_0)$ is still hermitian, and is a fiducial projector. The images $u_p' := \sigma(u_p)$ are correlations for P_0' and hence satisfy (10.8). □

The following condition requires that all the other Galois conjugates $\sigma(u_p)$ of u_p are real.

Definition 10.22. *A fiducial projector P_0 is called strong if, for all p in $(\mathbb{Z}/d'\mathbb{Z})^2$, the correlation u_p belongs to $\mathbb{E}_1$*

Remark 10.23. This condition heavily depends on the choice of the fiducial projector P_0 in a given HSIC. Indeed replacing P_0 by $P_0' := D_q P_0 D_q^{-1}$ with $2q \not\equiv 0$ mod d, replaces the correlations u_p by the correlations

$$u_p' \ = \ \mathrm{tr}(P_0' D_p) \ = \ \mathrm{tr}(P_0 D_q^{-1} D_p D_q) \ = \ \zeta_d^{p_2q_1 - p_1q_2} u_p.$$

But, for suitable p, the factor $\zeta_d^{p_2q_1 - p_1q_2}$ does not belong to $\mathbb{E}_1$ since it has no real Galois conjugate.

Definition 10.24. *A fiducial projector* $P_0 = |v_0\rangle\langle v_0|$ *is centred if* $Zv_0 = v_0$ *where* Z *is the Zauner matrix. It is strongly centred if moreover it is strong.*

The following conjecture is a technical but useful improvement of Conjectures 9.23 and 9.25 on the symmetry of order 3 in HSICs.

Conjecture 10.25. (a) *The set* $\mathcal{F}_{d,h}$ *is not empty and every* PEN_d*-orbit in* $\mathcal{F}_{d,h}$ *contains a strongly centred fiducial projector.*
(b) *When* d *is coprime to* 3*, every centred fiducial projector is strongly centred.*

Let $z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$. We denote by $A_{d'}$ the abelian subring,

$$A_{d'} = (\mathbb{Z}/d'\mathbb{Z})[z] \subset \mathcal{M}(2, \mathbb{Z}/d'\mathbb{Z})$$

and by $A^*_{d'}$ the group of units, or invertible elements in the ring $A_{d'}$.

Exercise 10.26. Prove that $A_{d'}$ is the centralizer of z in $\mathcal{M}(2, \mathbb{Z}/d'\mathbb{Z})$.

We introduce the subgroup $S := \{a \in A^*_{d'} \mid u_{ap} = u_p \text{ for all } p \in (\mathbb{Z}/d'\mathbb{Z})^2\}$. When d is odd, the subgroup S contains the group of order 3 generated by z. When d is even, the subgroup S contains the group of order 6 generated by z and $1 + d$. In most cases, the subgroup S is not larger.

In the following Conjecture 10.27, the precise choice of the factor $\eta_d^{p_1 p_2}$ in the definition of the displacement operators D_p is crucial.

Conjecture 10.27. *Assume the fiducial projector* P_0 *to be strongly centred. Assume also that* $f' = f$*.*
(a) *One has* $\mathbb{E}_0 \subset \mathbb{E}_1$*, and for all* $\sigma \in \mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$*, there exists* $a_\sigma \in A^*_{d'}$ *such that, for all* $p \in (\mathbb{Z}/d'\mathbb{Z})^2$*,* $\sigma(u_p) = u_{a_\sigma(p)}$*.*
(b) *The map* $\sigma \mapsto a_\sigma$ *induces an isomorphism* $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \xrightarrow{\simeq} A^*_{d'}/S$*.*

Remark 10.28. One can probably weaken the assumption $f' = f$. This assumption fits with the interpretation of these conjectures in terms of Class Field theory. Recall that the multiplet $[[P_0]]$ is associated to a ring $\mathcal{O}_{f'}$ of conductor f'. We will see that the group involved in Class Field Theory is the multiplicative group of the ring $\mathcal{O}_{f'}/d'\mathcal{O}_{f'}$ But since $\mathcal{O}_f = \mathbb{Z}[\varepsilon_d] = \mathcal{O}_{f'}$, one has an isomorphism of rings $A_{d'} = \mathcal{O}_f/d'\mathcal{O}_f = \mathcal{O}_{f'}/d'\mathcal{O}_{f'}$.

Example 10.29. When d is prime, $d \equiv 2 \bmod 3$, all the u_p, $p \neq 0$, are Galois conjugate over $\mathbb{E}_0$.

Indeed in this case, the ring A_d is the field $\mathbb{F}_{d^2}$ with d^2 elements.

Example 10.30. When d is prime, $d \equiv 1 \bmod 3$, The group $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ has exactly three orbits among the u_p, $p \neq 0$, one for each of the two z-invariant lines in $(\mathbb{Z}/d\mathbb{Z})^2$, and one for the complementary of these two lines.

Indeed in this case, the ring A_d is the product $\mathbb{F}_d \times \mathbb{F}_d$ of two copies of the field $\mathbb{F}_d = \mathbb{Z}/d\mathbb{Z}$.

Lemma 10.31. *We assume Conjecture 10.27. Let P_0 be a strongly centered fiducial projector. Then the field $\mathbb{E}_1$ is generated over $\mathbb{E}_0$ by the correlations u_p with p in $(\mathbb{Z}/d'\mathbb{Z})^2$.*

Proof. The injectivity of the map $\sigma \mapsto a_\sigma$ in Conjecture 10.27.b, tells us that every element σ in $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ that preserves the correlations u_p is trivial. By Galois theory, the field $\mathbb{E}_1$ is the smallest extension of $\mathbb{E}_0$ that contains all the correlations u_p. □

10.5 The phases as units

We recall that an algebraic unit is an algebraic integer whose inverse is also an algebraic integer.

We write $u_p = e^{i\theta_p}/\sqrt{p+1}$. The square of the phases

$$U_p := e^{2i\theta_p} = (d+1)u_p^2$$

depend only on p in $(\mathbb{Z}/d\mathbb{Z})^2$. Since P_0 is hermitian, the complex numbers U_p have absolute value 1.

Conjecture 10.32. *Let P_0 be a strongly centred fiducial projector.*
Then the complex numbers U_p are algebraic units.

Remark 10.33. Recall that all the Galois conjugates of U_p over $\mathbb{K}$ have modulus 1, and that, since P_0 is strongly centred, all the other Galois conjugates of U_p over $\mathbb{Q}$ are real and positive.

In this lecture we have stated striking arithmetic conjectures on HSICS using only Galois theory. We will need to use Class Field Theory to improve these conjectures. Indeed, given a number field $\mathbb{K}$ and an abelian extension $\mathbb{E}/\mathbb{K}$, knowing the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is a very weak information on this extension. For instance, all the quadratic extensions of $\mathbb{K}$ have the same Galois group $\mathbb{Z}/2\mathbb{Z}$. Class field theory gives a nice parametrization of the abelian extension of $\mathbb{K}$. Hence it will allow to predict exactly the fields $\mathbb{E}_0$, $\mathbb{E}_1$ and $\mathbb{E}$ associated to a multiplet $[[P_0]]$ of fiducial projectors.

Notes to Chapter 10.

The fields (10.1) where introduced by Appleby, Flammia, McConnel and Yard in [7, Sec. 4].

See also [46, Sec. 14] or [20] for two surveys on SICs.

11 Zauner example

In this lecture, we explicitely describe the 5-dimensional Heisenberg SICs. We will omit the computational proof. But we will check on this example the conjectures of the previous lecture.

11.1 The 5-dimensional HSIC

Let $d = d' = 5$. We denote by E and F the two $d \times d$ unitary matrices given by $E = (\delta_{j,k+1})$ and $F = (\zeta^j \delta_{j,k})$, where $\zeta = \zeta_d = e^{2i\pi/d}$. For $p = (p_1, p_2)$ in $(\mathbb{Z}/d'\mathbb{Z})^2$, we set $D_p = \eta_d^{p_1 p_2} E^{p_1} F^{p_2} \in \mathrm{U}(5)$. Recall the notation $\eta_d = -e^{i\pi/d}$. Here, $\eta_d = \zeta^{-2}$.

We are looking for a fiducial vector v_0, that is for a vector whose correlations $u_p := \frac{\langle v_0 | D_p v_0 \rangle}{\langle v_0 | v_0 \rangle}$ satisfy $|u_p| = \frac{1}{\sqrt{d+1}}$, for $p \neq 0$. Moreover we require that this fiducial vector $v_0 = (z_0, z_1, z_2, z_3, z_4)$ is invariant by the Zauner matrix. We normalize it by $z_0 = 1$. All the calculation can be done explicitely by hand because the eigenvalue 1 for the Zauner matrix has multiplicity 2. An explicit formula for v_0 can already be found in Zauner PhD thesis. We write $\zeta = e^{2i\pi/5} = c + is$, $\zeta' = e^{4i\pi/5} = c' + is'$, with c, s, c', s' real.

Lemma 11.1. *(Formulas for the Z-invariant fiducial vectors) The four vectors $v_0 := (z_0, z_1, z_2, z_3, z_4)$ given by $z_0 = 1$,*

$$\begin{aligned}
z_1 + z_4 &= \zeta^{-1}\left((1 - s') + c'\sqrt{3}\right) \\
(z_1 - z_4)^2 &= \zeta^{-2}\frac{(1 \pm 2i)}{\sqrt{5}}(2 + \sqrt{3})\left((1 - c)\sqrt{3} - s\right) \\
z_2 + z_3 &= \zeta\left((1 + s') + c'\sqrt{3}\right) \\
(z_2 - z_3)^2 &= \zeta^{2}\frac{(1 \pm 2i)}{\sqrt{5}}(2 + \sqrt{3})\left((1 - c)\sqrt{3} + s\right),
\end{aligned}$$

with the sign compatibility given by $\frac{z_1 - z_4}{z_3 - z_2}\zeta^2 = 1 + c + s\sqrt{3}$, are Z-invariant fiducial vector in $\mathbb{C}^5$. The square of the norm of these vectors v_0 is given by $N = \langle v_0 | v_0 \rangle = (3 - \sqrt{3})(5 - \sqrt{5})/2$.

These are exactly all the Z-invariant fiducial vectors.

We can then compute the correlations

Lemma 11.2. *(Formula for the correlations) The correlation*

$$u_0 := \frac{\langle v_0|Fv_0\rangle}{\langle v_0|v_0\rangle} = \frac{1}{N}\sum_{0\leqslant k\leqslant 4} \zeta^k |z_k|^2$$

of this fiducial vector is given by $u_0 = x_0 + iy_0 = e^{i\theta_0}/\sqrt{6}$ *where*

$$x_0 := \tfrac{1}{\sqrt{6}}\cos(\theta_0) \quad \text{is equal to} \quad x_0 = \tfrac{1}{4}\left((s'+c')\sqrt{5/3} + s' - c'\right)$$

$$y_0^2 := \tfrac{1}{6}\sin(\theta_0)^2 \quad \text{is equal to} \quad y_0^2 = \tfrac{1}{24}\left((1-c)\sqrt{3} + s\right).$$

The lengthy proof of Lemmas 11.1 and 11.2 are omitted.

Remark 11.3. Since v_0 is Z-invariant, the correlation u_0 is also $u_0 = \frac{\langle v_0|Ev_0\rangle}{\langle v_0|v_0\rangle}$.

11.2 The fields of the 5-dimensional HSIC

We can now compute the fields that are associated with this fiducial projector $P_0 = |v_0\rangle\langle v_0|$ and check the various conjectures of this lecture.

⋆ One has $\mathbb{K} = \mathbb{Q}[\sqrt{3}]$. Indeed, the Zauner unit is $\varepsilon_d = 2+\sqrt{3}$ and the discriminant is $\Delta_d = 12$.
⋆ The fundamental discriminant is $D_0 = 12$ and the conductor is $f = 1$.
⋆ This agrees with the fact that there is only one multiplet $[[P_0]]$.

⋆ One has $\mathbb{E}_0 := \mathbb{Q}[\sqrt{3}]$.
⋆ This agrees with the fact that $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}]$ is a principal ideal ring or equivalently the class number $h(\mathcal{O}_{\mathbb{K}}) = 1$. This fact follows from Minkowski's bound for the class number applied to $\mathbb{K}$: $h(\mathcal{O}_{\mathbb{K}}) \leqslant \sqrt{D_0}/2$.
⋆ This also agrees with the fact that there is only one geometric class $[P_0]$.

⋆ One has $\mathbb{E} := \mathbb{Q}[y_0, i]$.
⋆ One has $\mathbb{E}_1 := \mathbb{Q}[u_0] = \mathbb{Q}[iy_0]$ which is a quadratic extension of $\mathbb{Q}[\sqrt{3}, s]$.
⋆ We will check in Lemma 11.8 that the extension $\mathbb{E}_1/\mathbb{E}_0$ is Galois with cyclic Galois group $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \simeq \mathbb{Z}/8\mathbb{Z}$.
⋆ This agrees with the fact that the ring $A_{d'} = \mathbb{F}_5[z]$ is the field $\mathbb{F}_{25}$, hence has a cyclic multiplicative group with quotient group $\mathbb{F}_{25}^*/\langle z\rangle \simeq \mathbb{Z}/8\mathbb{Z}$.

⋆ There are $2000 = 80 \times 25$ fiducial projectors and 80 HSICs.
⋆ This agrees with the fact that, the group $\mathrm{PEN}_d \simeq \mathrm{SL}^{\pm}(2,\mathbb{F}_5) \ltimes \mathbb{F}_5^2$ has order 240×25, it acts transitively on $[P_0]$, and the stabilizer of P_0 is the group of order 3 generated by the Zauner matrix.

11.3 Galois action on correlations

In this section, we will explain graphically the action of the Galois group $\mathbb{Z}/8\mathbb{Z}$ on the correlations u_p. We will use a nice and fun graphic presentation of the field $\mathbb{F}_{25}$.

We choose now a generator σ of $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ so that $\sigma(\zeta) = \zeta^2$. For $\ell \in \mathbb{Z}/24\mathbb{Z}$, we set $u_\ell := \sigma^\ell(u_0)$, and one write $u_\ell = x_\ell + iy_\ell$. One has

$$u_{\ell+4} = \overline{u_\ell} \text{ and hence } u_{\ell+8} = u_\ell.$$

As above we identify the plane $(\mathbb{Z}/5\mathbb{Z})^2$ with the finite field $\mathbb{F}_{25}$ thanks to the bijection $(p_1, p_2) \longleftrightarrow p_1 + p_2\omega$ where $\omega^2 = -\omega - 1$. We introduce the generator $g_0 := 2 - 2\omega$ of the multiplicative group $\mathbb{F}_{25}^*$. We set $u_{p_\ell} := u_\ell$ where p_ℓ is the point corresponding to g_0^ℓ.

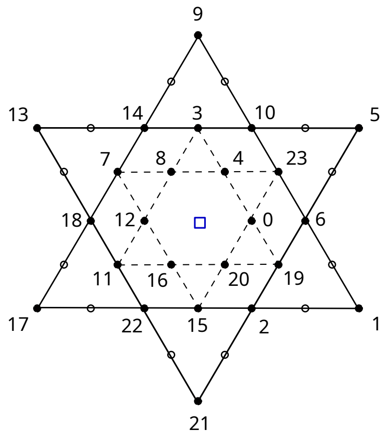


Figure 1: The field $\mathbb{F}_{25}$ seen as a labelled double star of David

In Figure 1, we have identified $\mathbb{F}_{25} = \mathbb{F}_5[\omega]/(\omega^2 + \omega + 1)$ with the quotient $R/5R$ where R is the ring $R = \mathbb{Z}[e^{2i\pi/3}] \subset \mathbb{C}$. For each of the 25 elements of $\mathbb{F}_{25}$, we have chosen a lift in R.

Since the multiplicative group $\mathbb{F}_{25}^*$ is cyclic of order 24 with generator $g_0 := 2 - 2\omega$, we can label the element g_0^k with the integer $k \in \mathbb{Z}/24\mathbb{Z}$. For instance, g_0 is labelled by 1, ω is labelled by 8, -1 is labelled by 12, 1 is labelled by 0, and … 0 is labelled by a blue square □.

By construction the multiplication in this graphic is nothing but the multiplication in $\mathbb{C}$ followed by a reduction modulo 5.

For instance, the multiplication by $-\omega^2$ in $\mathbb{F}_{25}$ is adding 4 on the labels which is turning by $\pi/3$ in the complex plane. The multiplication by 2 in $\mathbb{F}_{25}$ is adding 6 on the labels and is a homothety of ratio 2 on the small star and $-1/2$ on the large star. The action of the Frobenius in $\mathbb{F}_{25}$ is multiplying the labels by 5 which is the complex conjugation in the complex plane.

In this graphic the non-squares of $\mathbb{F}_{25}$ are the extremities of the branches of the stars and the squares are the multiples of the cubic roots of unity. We have also drawn the twelve affine lines over $\mathbb{F}_5$ that are parallel to one of the cubic roots of unity and do not contain 0.

The six $\mathbb{F}_5$ vector lines of $\mathbb{F}_{25}$ are the traces of six real lines containing 0 in the complex plane. We have not drawn them.

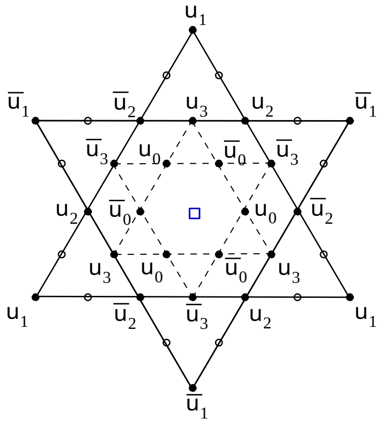


Figure 2: The correlations of the 5-dimensional SIC

In Figure 2, we show the correlations $u_p = \frac{\langle v_0 | D_p v_0\rangle}{\langle v_0 | v_0\rangle}$ of the 5-dimensional HSIC for a centred fiducial projector P_0, where the plane $(\mathbb{Z}/5\mathbb{Z})^2$ of parameters p is identified with $\mathbb{F}_{25}$. We have writen u_ℓ as a shortcut for $u_{g_0^\ell}$. The partial Fourier transform on the twelve affine lines is used to reconstruct the fiducial vector in Formulas (11.3).

Remark 11.4. The orthogonal projector on v_0 is given by the matrix

$$P_0 = (p_{j,k}) = \tfrac{1}{N^2}(z_j \overline{z}_k)$$

where $N = \|v_0\|$. The correlations u_p are given by the formula $u_p = tr(P_0 D_p)$, that is

$$u_{j+k\omega} = \textstyle\sum_\ell \zeta^{k(\ell-2j)} p_{\ell,j+\ell}. \tag{11.1}$$

Conversely, inverting this linear system, give the equalities

$$p_{j,k} = \tfrac{1}{5} \textstyle\sum_\ell \zeta^{2(j+k)\ell} u_{k-j+\ell\omega}. \tag{11.2}$$

In particular, if one normalizes v_0 by the condition $z_0 = 1$, one can recover the fiducial vector from the correlations: for $1 \leqslant j \leqslant 4$, one has

$$z_j = \tfrac{N}{5} \textstyle\sum_\ell \zeta^{2j\ell} u_{-j+\ell\omega}. \tag{11.3}$$

11.4 Finding the fiducial from an approximation

There is another approach that can be used to get algebraic formulas for the fiducial vectors for d small that works beyond $d = 5$ relying both on the conjectural predictions of this lecture and on a computer algebra system as Sagemath, Maple or Mathematica.

One first gets a 100 or 200-digits approximate values for a Z-invariant fiducial vector v_0 thanks to the gradient flow or to the Newton method as in Section 9.2. One then deduce approximate values for all the correlations $u_p = x_p + iy_p$.

Using again computer algebra, one wants to find the minimal polynomial of a correlation u_{p_0} over $\mathbb{Q}$ and to factorize it over the field $\mathbb{K}[\eta_d]$. This polynomial is quite huge and has large degree (degree 16 for $d = 5$). One may simplify a little bit the calculation, by first looking at the minimal polynomial over $\mathbb{Q}$ of $y_{p_0}^2$, which has smaller degree. One can also simplify the calculation since we can guess the list of all the Galois conjugate of u_{p_0} over $\mathbb{K}$ among the u_p, and since we have good numerical approximation for these u_p.

Once we have an algebraic formula for the correlations u_p, we obtain an algebraic formula for the fiducial vector v_0 thanks to a Formula as (11.3).

We finally can check rigorously using once more computer algebra that v_0 is indeed a fiducial vector.

11.5 A few cyclic extensions

In this section, we explain how to check directly that the extension $\mathbb{E}_1/\mathbb{K}$ for the 5-dimensional HSIC that we described in the previous section is indeed Galois with cyclic Galois group isomorphic to $\mathbb{Z}/8\mathbb{Z}$.

We first begin by a lemma which is a general but standard exercise in Galois theory.

Lemma 11.5. *Let k_0 be a field of characteristic $\neq 2$, k an abelian extension of k_0 with a cyclic Galois group G_0, and σ a generator of G_0. Let $Y \in k$ which is not a square in k, $y = \sqrt{Y}$ and $K := k[y]$.*
(a) K is a Galois extension of k_0 if and only if the ratio $\sigma(Y)/Y$ is a square in k.
(b) In this case the Galois group $G := \mathrm{Gal}(K/k_0)$ is abelian.
(c) In this case G is cyclic if and only if the norm $N_{k/k_0}(Y)$ is not a square in k_0.

Here is a very concrete application to quadratic and biquadratic extensions.

Corollary 11.6. *Let k_0 be a field of characteristic $\neq 2$, $d \in k_0$ non square and $k = k_0[\sqrt{d}]$. Let $Y = a + b\sqrt{d} \in k$ and $y = \sqrt{Y}$, $N := a^2 - db^2$, $K := k_0[y]$, L the Galois closure of K over k_0 and $G := \mathrm{Gal}(L/k_0)$.*
(a) One has the equivalences: $[K : k_0] = 4 \Longleftrightarrow Y$ is not a square in $k \Longleftrightarrow$
if $N = c^2$ with $c \in k_0$ then $(a \pm c)/2$ are not squares in k_0.
(b) Three cases are then possible:
(i) $G = (\mathbb{Z}/2\mathbb{Z})^2 \Longleftrightarrow N$ is a square in k_0.
(ii) $G = \mathbb{Z}/4\mathbb{Z} \Longleftrightarrow Nd$ is a square in k_0.
(iii) $G = D_4 \Longleftrightarrow$ neither N nor Nd are squares in $k_0 \Longleftrightarrow L \neq K$.

Here D_4 is the dihedral group with 8 elements $D_4 = (\mathbb{Z}/2\mathbb{Z}) \ltimes (\mathbb{Z}/4\mathbb{Z})$.

Exercise 11.7. Determine the Galois group $G_k = \mathrm{Gal}(L_k/\mathbb{Q})$ where L_k is the Galois closure of the field $K_k = \mathbb{Q}[y_k]$ for the following six values of y_k.
$y_1 = \sqrt{4 + \sqrt{15}}$, $y_2 = \sqrt{1 + i\sqrt{15}}$,
$y_3 = \sqrt{2 - \sqrt{2}}$, $y_4 = \sqrt{5 + \sqrt{5}}$,
$y_5 = \sqrt{1 + \sqrt{15}}$, $y_6 = \sqrt{1 + 4i\sqrt{3}}$.
Indication: $G_1 \simeq G_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$,
$G_3 \simeq G_4 \simeq \mathbb{Z}/4\mathbb{Z}$,
$G_5 \simeq D_4$, $G_6 \simeq \mathbb{Z}/2\mathbb{Z}$.

11.6 The correlation field for d=5

For $d = 5$, we have seen that there is essentially only one Z-invariant fiducial projector P_0. We have computed $\Delta_d = (d+1)(d-3) = 12$, and we have seen that $\mathbb{E}_0 = \mathbb{K} = \mathbb{Q}[\sqrt{3}]$. We also have computed explicitely the correlations $u_\ell := x_\ell + iy_\ell = e^{i\theta_\ell}/\sqrt{6}$ corresponding to a point g_0^ℓ. Those are the 8 Galois conjugates over $\mathbb{K}$ of an explicit element $u_0 = x_0 + iy_0$ with x_0 and $Y_0 := 24y_0^2$ in $\mathbb{K}[s]$ where $s := \sin(2\pi/5)$. The minimal polynomial over $\mathbb{K}$ of this element Y_0 is

$$Y^4 - 5\sqrt{3}\,Y^3 + 25\,Y^2 + 15\sqrt{3}\,Y + 5 = 0\,.$$

We have checked that $\mathbb{E}_1 = \mathbb{Q}[u_0] = \mathbb{Q}[iy_0]$. In the following lemma we explicitely check the general Conjecture 10.27 describing the Galois group $\mathrm{Gal}(\mathbb{E}_1/\mathbb{K})$. on this example with $d = 5$. We denote by Y_0, Y_1, Y_2, Y_3 the Galois conjugates of Y_0 over $\mathbb{E}_0$.

Lemma 11.8. (a) *The field* $\mathbb{L}_1 := \mathbb{E}_0[s]$ *is an abelian extension of degree* 8 *of* $\mathbb{Q}$. *One has* $\mathrm{Gal}(\mathbb{L}_1/\mathbb{Q}) \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ *and* $\mathrm{Gal}(\mathbb{L}_1/\mathbb{E}_0) \simeq \mathbb{Z}_4$.
(b) *The elements* Y_0, Y_1, Y_2 *and* Y_3 *are positive and* $-Y_0$, $-Y_1$, $-Y_2$ *et* $-Y_3$ *are the other Galois conjugate of* Y_0 *over* $\mathbb{Q}$.
(c) *The field* $\mathbb{E}_1 = \mathbb{Q}[u_0]$ *is a quadratic extension of* $\mathbb{L}_1$ *equal to* $\mathbb{L}_1[iy_0]$. *This field* $\mathbb{E}_1$ *is an extension of* $\mathbb{Q}$ *of degree* 16 *which is not Galois.*
(e) *The field* $\mathbb{E}_1$ *is an abelian extension of* $\mathbb{K}$, *and one has* $\mathrm{Gal}(\mathbb{E}_1/\mathbb{K}) \simeq \mathbb{Z}_8$.

Sketch of proof. (a) The field $\mathbb{L}_1$ is cyclotomic.

(b) This follows from the explicit formula for Y_0 given in Lemma 11.2.

(c) The first sentence follows from the explicit formula for u_0 also given in Lemma 11.2.

The field $\mathbb{E}_1$ is not Galois over $\mathbb{Q}$ because the image $\mathbb{E}_2 = \sigma_0(\mathbb{E}_1)$ of $\mathbb{E}_1$ by an element $\sigma_0 \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ such that $\sigma_0(\sqrt{3}\,) = -\sqrt{3}$ is the field $\mathbb{E}_2 = \mathbb{Q}[y_0] \subset \mathbb{R}$, while the field $\mathbb{E}_1$ is not a subfield of $\mathbb{R}$.

(d) The key point is to notice the two equalities

$$Y_1/Y_0 = (2\sqrt{3} + Y_0)^2 \quad \text{and} \quad Y_0Y_1Y_2Y_3 = 5$$

and to apply Lemma 11.5. □

Exercise 11.9. **On the field of definition of the 6-dimensional HSIC.** Let $\omega = e^{2i\pi/3}$, $\mathbb{K} = \mathbb{Q}[\sqrt{21}]$ and $\mathbb{F} = \mathbb{K}[x]$ where $x \in \mathbb{C}$ satisfies $x^3 = 1 + i\sqrt{7}$.
A) a) Compute $x\overline{x}$ and prove that x is an algebraic integer.
b) Prove that x does not belong to $\mathbb{Q}[i\sqrt{7}]$.
c) Prove that $\mathbb{Q}[x]$ is an extension of degree 6 of $\mathbb{Q}$.
d) Prove that $\mathbb{F}$ is an extension of degree 12 of $\mathbb{Q}$.
e) Prove that $\mathbb{F}$ is a Galois extension of $\mathbb{Q}$.
B) a) Prove that there exists $\rho \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ such that $\rho(x) = \omega\overline{x}$.
b) Prove that $\rho(\omega) = \omega^2$, that $\rho^2(x) = \omega x$ and that $\rho^3(x) = \overline{x}$.

c) Prove that $\mathbb{F}$ is a cyclic extension of $\mathbb{K}$ of degree 6.
d) Prove that the group $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ is a dihedral group of order 12.
e) Since this field $\mathbb{F}$ is included in the field $\mathbb{E}$ of definition of the unique 6-dimensional HSIC, how does this exercise fit with the conjectures on HSICs?

In section 11.1 The existence of the 5 dimensional HSIC with explicit formulas is due to Zauner in his PhD thesis [47]. See also the more recent paper by Appleby and Bengsston [5] which gives more details on the fields involved. In section 11.5

12 Class field theory

Most of this lecture, is a survey with no proof of Class Field Theory. This theory classifies abelian extensions of global or local fields. It began in the middle of the 19th century by the characterization, due to Kronecker and Weber, of the cyclomotomic fields as the abelian extensions of $\mathbb{Q}$. One of the main original motivation of Class Field Theory is the extension of this theorem over more general number fields $\mathbb{K}$ than the rationals, as in "Kronecker youth dream" where $\mathbb{K}$ is an imaginary quadratic field. A first achievement in the early 20th century is the construction of the maximal unramified abelian extension called the Hilbert class field.

The abelian extensions that occur in SICs are ramified. Fortunately, a second achievement of Class Field Theory due to Takagi allows to deal with abelian extensions that are ramified. A third achievement is a class field theory over local fields. This allows to deduce Global Class Field Theory by gathering together the Local Class Field Theories for all the completions of $\mathbb{K}$ thanks to the language of adèles and idèles.

12.1 Unramified class field theory

We begin by the case of the maximal unramified abelian extension which is called the Hilbert class field. This case is already very useful.

Let $\mathbb{K}$ be a global field. In characteristic zero, this means a number field. In characteristic p, this means a finite extension of the field $\mathbb{F}_p(t)$ of rational functions. Let $\mathcal{O}_\mathbb{K}$ be the ring of integers of $\mathbb{K}$, which is the integral closure in $\mathbb{K}$ of either $\mathbb{Z}$ or $\mathbb{F}_p[t]$.

Ideal class group One recall that the class group $\mathcal{C}l(\mathcal{O}_\mathbb{K}) = \mathrm{Pic}(\mathcal{O}_\mathbb{K})$ of a number field $\mathbb{K}$ is the group of class of ideals in the ring of integers $\mathcal{O}_\mathbb{K}$ modulo the principal ideals. The class number $h(\mathcal{O}_\mathbb{K})$ of $\mathbb{K}$ is the cardinality of this group.

A conjecture of Cohen and Lenstra states that about 75% of the real quadratic fields $\mathbb{Q}[\sqrt{p}]$ with p prime have a trivial class group. One does not know neither if the set of such primes p is finite, nor if its complementary is finite.

When d is square free and composite, then $\mathbb{Q}[\sqrt{d}]$ often has a non-trivial class group. This is the case for $\mathbb{Q}[\sqrt{10}]$ or $\mathbb{Q}[\sqrt{15}]$ and more generally when

d has a prime factor $p \equiv 1 \bmod 4$.

Ramification One recall that an extension $\mathbb{L}$ of $\mathbb{K}$ is unramified if
- it is unramified at finite places, that is, for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$, the ring $\mathcal{O}_{\mathbb{L}}/\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ does not have zero divisors,
- it is unramified at infinite places, that is, each time a completion $\mathbb{K}_v$ is equal to $\mathbb{R}$ the completions $\mathbb{L}_w$ extending it are also equal to $\mathbb{R}$.

In the case where $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}[\alpha]$ and the ring of integer is monogenous $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\alpha]$, the extension $\mathbb{L}/\mathbb{Q}$ is ramified at a prime p if and only if p divides the discriminant of the minimal polynomial of α on $\mathbb{Z}$. In particular every extension of $\mathbb{Q}$ is ramified.

Example For d square free, $\mathbb{Q}[\sqrt{d}]$ is ramified exactly:
(i) at the prime divisors p of d,
(ii) at $p = 2$ when $d \not\equiv 1 \bmod 4$, and
(iii) at $p = \infty$ when $d < 0$.

Hilbert class fields There exists a unique maximal unramified abelian extension $\mathbb{L}$ of $\mathbb{K}$. According to class field theory this is a finite extension of $\mathbb{K}$ and one can describe its Galois group in the following way:

For every prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$, the quotient $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ is a finite field $\mathbb{F}_q$. Since the extension $\mathbb{L}/\mathbb{K}$ is unramified, the finite ring $\mathcal{O}_{\mathbb{L}}/\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ is a product of finite fields $\mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i$ where the $\mathfrak{P}_i$ are, by definition, the prime ideals of $\mathcal{O}_{\mathbb{L}}$ that divide $\mathfrak{p}$. These prime ideals are exchanged under the action of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

There exists an element $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ that preserves such a prime $\mathfrak{P}_i$ and acts on the finite quotient field $\mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i$ as the Frobenius $x \mapsto x^q$. Since all these primes $\mathfrak{P}_i$ are Galois conjugate and since the extension $\mathbb{L}/\mathbb{K}$ is abelian this element $\sigma_{\mathfrak{p}}$ is unique and is called the Frobenius at $\mathfrak{p}$.

The map $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$ induces an isomorphism, denoted Art, of abelian groups

$$\mathrm{Art} : \mathcal{C}l(\mathcal{O}_{\mathbb{K}}) \simeq \mathrm{Gal}(\mathbb{L}/\mathbb{K}).$$

This extension $\mathbb{L}$ is called the Hilbert class field of $\mathbb{K}$.

In particular, when $\mathcal{O}_{\mathbb{K}}$ is principal, every abelian extension of $\mathbb{K}$ is ramified.

Exercise 12.1. a) Check that the ring of integers $\mathbb{Z}[\sqrt{15}]$ is not principal.
a) Check that the abelian extension $\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q}[\sqrt{15}]$ is unramified.

12.2 Local class field

Let K be a local field. In characteristic zero, this means a finite extension of a p-adic field $\mathbb{Q}_p$. In characteristic p, this means a finite extension of the field $\mathbb{F}_p((t))$ of Laurent series.

The Local Class Field theory describe the maximal abelian extension K^{ab} of K and its Galois group. For every finite abelian extension L of K one introduce the norm map $N_{L/K}$ which is the multiplicative groups morphism

$$\begin{array}{rcl} N_{L/K} : L^* & \longrightarrow & K^* \\ x & \mapsto & N_{L/K}(x) = \det_L(m_x) = \prod_\sigma \sigma(x), \end{array}$$

where $m_x \in \mathrm{End}_K(L)$ is the multiplication by x, and where the product is over all $\sigma \in \mathrm{Gal}(L/K)$. We denote by $\mathcal{N}_L := N_{L/K}(L^*)$ the image in K^* of the norm map.

Theorem 12.2. *a) The map $L \to \mathcal{N}_L$ is a bijection between*

$$\left\{ \begin{array}{c} \textit{finite abelian} \\ \textit{extensions } L \textit{ of } K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{finite index open} \\ \textit{subgroups } \mathcal{N} \textit{ of } K^* \end{array} \right\}. \tag{12.1}$$

b) For L_1 and L_2 extension of K, one has the equivalence

$$L_1 \subset L_2 \Longleftrightarrow \mathcal{N}_{L_1} \supset \mathcal{N}_{L_2},$$

and the equalities

$$\begin{array}{rcl} \mathcal{N}_{L_1 \cap L_2} & = & \mathcal{N}_{L_1}\mathcal{N}_{L_2}, \\ \mathcal{N}_{L_1 L_2} & = & \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}. \end{array}$$

c) There exists a canonical isomorphism

$$\mathrm{Art} = \mathrm{Art}_K : K^*/\mathcal{N}_L \simeq \mathrm{Gal}(L/K) \tag{12.2}$$

called the Artin symbol.

Here are a few facts, remarks or exercises that help to understand how to deal with this group $K^*/\mathcal{N}_L$.

1. For $K = \mathbb{R}$ or $\mathbb{C}$, one sets $\mathcal{O}_K^* := K^*$. The trivial extension K/K is called unramified and it corresponds to the full subgroup $\mathcal{N}_K = K^*$. For $K = \mathbb{R}$, the extension $\mathbb{C}/\mathbb{R}$ is called ramified and it corresponds to the subgroup $\mathcal{N}_{\mathbb{C}} = \mathbb{R}_+^*$.

2. For K non archimedian, one denote by $\mathcal{O}_K$ its ring of integers, π a uniformizer, $\kappa = \mathcal{O}_K/\pi\mathcal{O}_K = \mathbb{F}_q$ the residual field where $q = p^\ell = |\kappa|$.
One has then

$$K^* = \pi^{\mathbb{Z}} \times \mathcal{O}_K^* = \pi^{\mathbb{Z}} \times (\mathbb{Z}/(q-1)\mathbb{Z}) \times (1 + \pi\mathcal{O}_K).$$

The group $(1 + \pi\mathcal{O}_K)$ has no torsion when $K = \mathbb{Q}_p$ with p odd.

Exercise 12.3. Let K be a local field of characteristic zero and L/K be an extension of degree n.
a) Prove that the group $\mathcal{N}_L$ contains the subgroup K^{*n}.
b) Prove that the subgroup K^{*n} is an open finite index subgroup of K^*

3. When K is non archimedean, an abelian extension L/K is called unramified if π is also an uniformizer for L. When K is archimedean, an abelian extension L/K is called unramified if $L = K$.

An abelian extension L/K is unramified if and only if $\mathcal{N}_L$ contains $\mathcal{O}_K^*$

4. When K is non archimedean, one denotes by K_n the unique unramified extension of degree n of K. Its residual field κ_n is the unique extension of degree n of the finite field κ. The field K_n is generated by the $(q^n-1)^{\text{th}}$ roots of unity. Hence it is an abelian extension of K. The union K^{nr} of these extensions is the maximal unramified abelian extension of K. One has

$$\mathcal{N}_{K_n} = \pi^{n\mathbb{Z}} \times \mathcal{O}_K^* \text{ and } K^*/\mathcal{N}_{K_n} = \mathbb{Z}/n\mathbb{Z}.$$

5. When $K = \mathbb{Q}_p$, one denotes by $L_n = \mathbb{Q}_p[\zeta_{p^n}]$ the field generated by the $p^{n\text{th}}$ roots of unity. It is a totally ramified abelian extension of degree $p^{n-1}(p-1)$ of $\mathbb{Q}_p$. One has

$$\mathcal{N}_{L_n} = \pi^{\mathbb{Z}} \times (1 + p^n\mathbb{Z}_p) \text{ and } K^*/\mathcal{N}_{L_n} = (\mathbb{Z}/p^n\mathbb{Z})^*.$$

Exercise 12.4. Prove using (12.1) that the extension $\mathbb{Q}_p^{ab}$ is generated by all the m^{th} roots of unity where $m \geqslant 1$.
Indication: Every finite index subgroup of $\mathbb{Q}_p^*$ contains a group of the form

$$p^{n\mathbb{Z}} \times (1 + p^n\mathbb{Z}_p).$$

Exercise 12.5. Let $K = \mathbb{Q}_5[\sqrt{3}] = \mathbb{Q}_5[\omega]$ with $\omega^2 + \omega + 1 = 0$ and $L = K[y]$ with

$$y^8 - 5\sqrt{3}y^6 + 25\,y^4 + 15\sqrt{3}\,y^2 + 5 = 0\,. \tag{12.3}$$

a) Check, using Eisenstein criterion, that L is an extension of degree 8 of K.
b) Check, using Lemma 11.8, that L is an abelian extension of K.
c) Check that $\mathcal{N}_L$ has index 8 in K^*.
d) Check that $N_{L/K}(y) = 5$ and that $(\mathcal{O}_K^*)^8 = \langle \omega, 1 + 5\mathcal{O}_K \rangle$.
e) Check that $\mathcal{N}_L = \langle 5, \omega, 1 + 5\mathcal{O}_K \rangle$.

12.3 Adèles

The link between local class field and global class field is the language of adèles and idèles due to Chevalley.

Let $\mathbb{K}$ be a number field, extension of degree n of $\mathbb{Q}$, and let $\mathcal{O}_\mathbb{K}$ be its ring of integers. We denote by v a place of $\mathbb{K}$ and $\mathbb{K}_v$ the corresponding completion of $\mathbb{K}$. The finite places are those corresponding to prime ideals of $\mathcal{O}_\mathbb{K}$. The infinite places are either real or complex. Let $\Sigma_{\mathbb{K},r}$ be the set of real places of $\mathbb{K}$. We write $n = r_1 + 2r_2$ where $r_1 = |\Sigma_{\mathbb{K},r}|$.

Let $\widehat{\mathcal{O}_\mathbb{K}} := \varprojlim_{d\infty} \mathcal{O}_\mathbb{K}/d\mathcal{O}_\mathbb{K}$ be the ring profinite limit of $\mathcal{O}_K$. The ring of finite adèle is the ring

$$A_{\mathbb{K},f} := \widehat{\mathcal{O}_\mathbb{K}} \otimes_\mathbb{Z} \mathbb{Q} = \prod_{v \text{ finite}}{}' \; \mathbb{K}_v$$

which is also equal to the restricted product of the completions $\mathbb{K}_v$, restricted with respect to the integers $\mathcal{O}_{\mathbb{K}_v}$. The ring of adèles is the product

$$A_\mathbb{K} := A_{\mathbb{K},f} \times A_{\mathbb{K},\infty} \; = \prod_v{}' \; \mathbb{K}_v \;\; \text{where}$$

$$A_{\mathbb{K},\infty} := \prod_{v \text{ infinite}} \mathbb{K}_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

The field $\mathbb{K}$ embeds diagonally in the ring of adèles. We quote with no proof the following

Proposition 12.6. *The additive group $\mathbb{K}$ is a discrete subgroup of the locally compact group $A_\mathbb{K}$ and the quotient $\mathbb{A}_\mathbb{K}/\mathbb{K}$ is compact and connected.*

12.4 Idèles

The group of idèles $I_{\mathbb{K}}$ is the multiplicative group of $A_{\mathbb{K}}$. It is a locally compact when seen as the closed subset

$$I_{\mathbb{K}} = \mathrm{GL}(1, A_{\mathbb{K}}) = \{(x,y) \in A_{\mathbb{K}}^2 \mid xy = 1\} \subset A_{\mathbb{K}}^2.$$

The group of idèles is also the restricted product of the multiplicative groups

$$I_{\mathbb{K}} = \prod_v{}' \mathbb{K}_v^* = I_{\mathbb{K},f} \times I_{\mathbb{K},\infty}$$

of all the completions $\mathbb{K}_v$ of $\mathbb{K}$, product restricted to the groups of units $\mathcal{O}_{\mathbb{K}_v}^*$ of $\mathbb{K}_v^*$. This means that an idèle $x = (x_v)$ has almost all its components x_v in $\mathcal{O}_{\mathbb{K}_v}^*$.

The absolute value $|x|$ of an idèle $x = (x_v)$ is the product of the absolute values $|x| := \prod_v |x_v|_v$. We set

$$I_{\mathbb{K}}^1 = \{x \in I_{\mathbb{K}} \mid |x| = 1\}.$$

The multiplicative group $\mathbb{K}^*$ is a subgroup of $I_{\mathbb{K}}$ via the diagonal embedding. The product formula tells us that $\mathbb{K}^*$ is included in $I_{\mathbb{K}}^1$.

Proposition 12.7. *The multiplicative group $\mathbb{K}^*$ is a cocompact discrete subgroup of the locally compact abelian group $I_{\mathbb{K}}^1$.*

Remark 12.8. This proposition encapsulates both the finiteness of the class group $\mathcal{C}l(\mathcal{O}_{\mathbb{K}})$ and the Dirichlet units theorem.

Definition 12.9. *The idèles class group is the quotient $C_{\mathbb{K}} := I_{\mathbb{K}}/\mathbb{K}^*$.*

Note that one has an exact sequence

$$1 \longrightarrow C_{\mathbb{K}}^1 \longrightarrow C_{\mathbb{K}} \longrightarrow \mathbb{R}_+^* \longrightarrow 1$$

where the group $C_{\mathbb{K}}^1 := I_{\mathbb{K}}^1/\mathbb{K}^*$ is compact.

In class field theory one is dealing with finite index open subgroups of $I_{\mathbb{K}}$ that contains $\mathbb{K}^*$. Those subgroups always contain the connected component $I_{\mathbb{K}}^0 = I_{\mathbb{K},\infty}^0 \simeq \mathbb{R}_+^{r_1} \times \mathbb{C}^{r_2}$. This is why the following exact sequence will be useful.

We introduce the 'unramified finite index open subgroup" of $I_{\mathbb{K}}$ to be the group

$$U_{\mathbb{K}} = \prod_v \mathcal{O}^*_{\mathbb{K}_v} = \widehat{\mathcal{O}_{\mathbb{K}}}^* \times \{\pm 1\}^{\Sigma_{\mathbb{K},r}} \times I^0_{\mathbb{K},\infty} \tag{12.4}$$

(we recall that, when $\mathbb{K}_v = \mathbb{R}$ or $\mathbb{C}$, by convention, one sets $\mathcal{O}^*_{\mathbb{K}_v} = \mathbb{K}^*_v$). One has

$$\mathbb{K}^* \cap U_{\mathbb{K}} = \mathcal{O}^*_{\mathbb{K}} \text{ and } \mathcal{C}l(\mathcal{O}_{\mathbb{K}}) = I_{\mathbb{K}}/(\mathbb{K}^* U_{\mathbb{K}}).$$

Hence one has the following exact sequence that allows us to better understand the idèles class group.

Lemma 12.10. *One has an exact sequence*

$$1 \longrightarrow \mathcal{O}^*_{\mathbb{K}} \longrightarrow U_{\mathbb{K}} \longrightarrow C_{\mathbb{K}} \longrightarrow \mathcal{C}l(\mathcal{O}_{\mathbb{K}}) \longrightarrow 1 \tag{12.5}$$

12.5 Global class field

Global Class Field theory describes the maximal abelian extensions $\mathbb{K}^{ab}$ of a global field $\mathbb{K}$ and its Galois group $\mathrm{Gal}(\mathbb{K}^{ab}/\mathbb{K})$.

For all finite extension $\mathbb{L}$ of $\mathbb{K}$ one introduces the norm map which is the group morphism given by

$$\begin{array}{rcl} N_{\mathbb{L}/\mathbb{K}} : I_{\mathbb{L}} & \longrightarrow & I_{\mathbb{K}} \\ x = (x_w) & \mapsto & y = (y_v) \text{ where } y_v := \prod_{w|v} N_{\mathbb{L}_w/\mathbb{K}_v}(x_w)\,. \end{array}$$

It extends the classical norm map $N_{\mathbb{L}/\mathbb{K}} : \mathbb{L}^* \longrightarrow \mathbb{K}^*$, and hence it induces a group morphism still called the norm map and denoted the same way $N_{\mathbb{L}/\mathbb{K}} : C_{\mathbb{L}} \longrightarrow C_{\mathbb{K}}$. We denote by

$$\mathcal{N}_L := N_{\mathbb{L}/\mathbb{K}}(C_{\mathbb{L}}) \subset C_{\mathbb{K}}$$

the image of this last norm map.

Theorem 12.11. *a) The map $\mathbb{L} \to \mathcal{N}_{\mathbb{L}}$ is a bijection between*

$$\left\{ \begin{array}{c} \textit{finite abelian} \\ \textit{extensions } \mathbb{L} \textit{ of } \mathbb{K} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{finite index open} \\ \textit{subgroups } \mathcal{N} \textit{ of } C_{\mathbb{K}} \end{array} \right\}. \tag{12.6}$$

b) For $\mathbb{L}_1$ and $\mathbb{L}_2$ extension of $\mathbb{K}$, one has the equivalence

$$\mathbb{L}_1 \subset \mathbb{L}_2 \Longleftrightarrow \mathcal{N}_{\mathbb{L}_1} \supset \mathcal{N}_{\mathbb{L}_2},$$

and the equalities

$$\begin{aligned}\mathcal{N}_{\mathbb{L}_1 \cap \mathbb{L}_2} &= \mathcal{N}_{\mathbb{L}_1}\mathcal{N}_{\mathbb{L}_2},\\ \mathcal{N}_{\mathbb{L}_1\mathbb{L}_2} &= \mathcal{N}_{\mathbb{L}_1} \cap \mathcal{N}_{\mathbb{L}_2}.\end{aligned}$$

c) The local Artin symbols $\mathrm{Art}_{\mathbb{K}_v} : \mathbb{K}_v^* \to \mathrm{Gal}(\mathbb{L}_w/\mathbb{K}_v)$ *induce an isomorphism*

$$\begin{aligned}\mathrm{Art}_{\mathbb{K}} : C_{\mathbb{K}}/\mathcal{N}_{\mathbb{L}} &\xrightarrow{\simeq} \mathrm{Gal}(\mathbb{L}/\mathbb{K})\\ x \bmod \mathcal{N}_{\mathbb{L}} &\mapsto \mathrm{Art}_{\mathbb{K}}(x) := \prod_v \mathrm{Art}_{\mathbb{K}_v}(x_v),\end{aligned} \tag{12.7}$$

where $x \in C_{\mathbb{K}}$ *is written as* $x = (x_v) \bmod \mathbb{K}^*$*.*

Here are a few facts, remarks or exercises that help to understand how to deal with this group $C_{\mathbb{K}}^*/\mathcal{N}_{\mathbb{L}}$.

1. Since the extension $\mathbb{L}/\mathbb{K}$ is abelian each group $\mathrm{Gal}(\mathbb{L}_w/\mathbb{K}_v)$ is canonically isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$: the decomposition subgroup for $w|v$

$$D_w := \{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \mid \sigma(w) = w\} \simeq \mathrm{Gal}(\mathbb{L}_w/\mathbb{K}_v)$$

which does not depend on the valuation w of $\mathbb{L}$ over v.

2. The product (12.7) is finite since, for almost all v, the element x_v is a unit of $\mathbb{K}_v$ and the extension $\mathbb{L}_w/\mathbb{K}_v$ is unramified and hence $\mathrm{Art}_{\mathbb{K}_v}(x_v) = 1$. The order in the product does not mind since $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is abelian.

3. The fact that the Artin map is trivial on $\mathbb{K}^*$ is a subtle point that we will be able to discuss only in Section 13.2 when we will have given a precise definition of the Artin symbols $\mathrm{Art}_{\mathbb{K}_v}$.

4. The subgroup $\mathcal{N}(\mathcal{O}_{\mathbb{K}}) := \mathbb{K}^* U_{\mathbb{K}}/\mathbb{K}^* \subset C_{\mathbb{K}}$ corresponds via (12.6) to the maximal unramified abelian extension of $\mathbb{K}$: this is the Hilbert class field of $\mathbb{K}$ that we discussed in Section 12.1

5. All the open subgroups of $C_{\mathbb{K}}$ contain the connected component $C_{\mathbb{K}}^0$. This tells us that, in dealing with open subgroups $\mathcal{N}$ of $C_{\mathbb{K}}$, we only have to deal with the finite places and to keep track of signs at the real places. This motivates the definition in the next section of the Ray class fields whose union will be $\mathbb{K}^{ab}$.

6. Roughly, Theorem 12.11.a tells us that to define an abelian extension $\mathbb{L}$ of a global field $\mathbb{K}$, you just need to choose the places where you allow ramification and to prescribe the level of ramification.

12.6 Ray class field of extended ideals

In this section, we define ray class fields associated to an extended invertible ideal $(\mathfrak{m}, \Sigma)$ of an order $\mathcal{O}$ of a number field $\mathbb{K}$. We will see in the next lecture that these ray class fields with $\mathbb{K} = \mathbb{Q}[\sqrt{\Delta_d}]$ are precisely the fields that occurs with d-dimensional HSICS.

A remarquable family of open subgroups of finite index of $I_{\mathbb{K}}$ are the principal subgroups $U_{\mathfrak{m},\Sigma}(\mathcal{O}) \subset U_{\mathbb{K}}$ defined as follows, see [42] or [27]. We fix an order $\mathcal{O} \subset \mathcal{O}_{\mathbb{K}}$, an ideal $\mathfrak{m}$ of $\mathcal{O}_{\mathbb{K}}$ and a subset $\Sigma \subset \Sigma_{\mathbb{K},r}$ of real places $\mathbb{K}$. Such a pair $(\mathfrak{m}, \Sigma)$ is called an extended ideal or a modulus.

To avoid a few technicalities, we will assume that the ideal $\mathfrak{m}$ is invertible. This means that there exists an ideal $\mathfrak{m}'$ of $\mathcal{O}$ such that the product ideal $\mathfrak{m}'\mathfrak{m}$ is a principal ideal of $\mathcal{O}$. This condition is automatic when $\mathcal{O} = \mathcal{O}_{\mathbb{K}}$. It is also satisfied for the ideals of the form $\mathfrak{m} = d\mathcal{O}$ for some integer $d \geqslant 1$ that occur when studying HSICs.

One has an embbeding of the profinite completions

$$\widehat{\mathfrak{m}} \subset \widehat{\mathcal{O}} \subset \widehat{\mathcal{O}_{\mathbb{K}}},$$

and the profinite completion $\widehat{\mathfrak{m}}$ is an ideal of $\widehat{\mathcal{O}}$ which is a subring of $\widehat{\mathcal{O}_{\mathbb{K}}}$.

One defines the open subgroup $U_{\mathfrak{m},\Sigma}(\mathcal{O})$ of the group $U_{\mathbb{K}} \subset I_{\mathbb{K}}$ introduced in (12.4)

$$U_{\mathfrak{m},\Sigma}(\mathcal{O}) = \widehat{\mathcal{O}}^*_{\mathfrak{m}} \times \{\pm 1\}^{\Sigma_{\mathbb{K},r} \smallsetminus \Sigma} \times I^0_{\mathbb{K},\infty}$$

where

$$\widehat{\mathcal{O}}^*_{\mathfrak{m}} = \{x \in \widehat{\mathcal{O}}^* \mid x \equiv 1 \bmod \widehat{\mathfrak{m}}\}$$

Definition 12.12. *We denote by $H_{\mathfrak{m},\Sigma}(\mathcal{O})$ the finite abelian extension of $\mathbb{K}$ associated by* (12.6) *to the open finite index subgroup*

$$\mathcal{N}_{\mathfrak{m},\Sigma}(\mathcal{O}) := \mathbb{K}^* U_{\mathfrak{m},\Sigma}(\mathcal{O})/\mathbb{K}^* \subset C_{\mathbb{K}}.$$

This field $H_{\mathfrak{m},\Sigma}(\mathcal{O})$ is called the Ray class field of the extended ideal $(\mathfrak{m}, \Sigma)$ of $\mathcal{O}$. The quotient group

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) := C_{\mathbb{K}}/\mathcal{N}_{\mathfrak{m},\Sigma}(\mathcal{O})$$

is called the Ray class group of the extended ideal $(\mathfrak{m}, \Sigma)$ of $\mathcal{O}$.

We still denote by Art all the isomorphisms given by the Artin map

$$\mathrm{Art} : \mathcal{C}l_{\mathfrak{m},\Sigma}(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{m},\Sigma}(\mathcal{O})/\mathbb{K}). \tag{12.8}$$

Remark 12.13. In these notations, we may omit the ideal $\mathfrak{m}$ when $\mathfrak{m} = \mathcal{O}$, we may omit the subset Σ when $\Sigma = \varnothing$, we may replace Σ by a $+$ when Σ is the full set $\Sigma = \Sigma_{\mathbb{K},r}$.

First example: the Hilbert class field
When $\mathcal{O} = \mathfrak{m} = \mathcal{O}_{\mathbb{K}}$ and $\Sigma = \varnothing$, the group $\mathcal{C}l(\mathcal{O}_{\mathbb{K}}) = \mathcal{C}l_{\mathcal{O}_{\mathbb{K}},\varnothing}(\mathcal{O}_{\mathbb{K}})$ is the class group of $\mathcal{O}_{\mathbb{K}}$ and the corresponding field $H(\mathcal{O}_{\mathbb{K}}) = H_{\mathcal{O}_{\mathbb{K}},\varnothing}(\mathcal{O}_{\mathbb{K}})$ is the Hilbert class field of $\mathbb{K}$. It is the maximal unramified abelian extension of $\mathbb{K}$.

Second example: the narrow Hilbert class field
When $\mathcal{O} = \mathfrak{m} = \mathcal{O}_{\mathbb{K}}$ and $\Sigma = \Sigma_{\mathbb{K},r}$, the group $\mathcal{C}l_+(\mathcal{O}_{\mathbb{K}}) = \mathcal{C}l_{\Sigma_{\mathbb{K},r}}(\mathcal{O}_{\mathbb{K}})$ is called the narrow class group of $\mathcal{O}_{\mathbb{K}}$ and the field $H_+(\mathcal{O}_{\mathbb{K}}) = H_{\Sigma_{\mathbb{K},r}}(\mathcal{O}_{\mathbb{K}})$ is called the narrow Hilbert class field of $\mathbb{K}$. It is the maximal abelian extension of $\mathbb{K}$ which is unramified at all the finite places. The narrow class group can be computed with the exact sequence

$$1 \to \mathcal{O}_{\mathbb{K}}^*/\mathcal{O}_{\mathbb{K},+}^* \to \{\pm 1\}^{\Sigma_{\mathbb{K},r}} \to \mathcal{C}l_+(\mathcal{O}_{\mathbb{K}}) \to \mathcal{C}l(\mathcal{O}_{\mathbb{K}}) \to 1 \tag{12.9}$$

where $\qquad \mathcal{O}_{\mathbb{K},+}^* := \{x \in \mathcal{O}_{\mathbb{K}}^* \mid x_v > 0 \text{ for all real place } v \text{ of } \mathbb{K}\}.$

Third example: the Hilbert class field of an order
When $\mathcal{O} = \mathfrak{m}$ and $\Sigma = \varnothing$, the group $\mathcal{C}l(\mathcal{O}) = \mathcal{C}l_{\mathcal{O},\varnothing}(\mathcal{O})$ is the group of classes of invertible ideals of $\mathcal{O}$ modulo the principal ideals, and the field $H(\mathcal{O}) = H_{\mathcal{O},\varnothing}(\mathcal{O})$ is the Hilbert class field of the order $\mathcal{O}$. The class group of $\mathcal{O}$ can be computed with the exact sequence

$$1 \to \mathcal{O}_{\mathbb{K}}^*/\mathcal{O}^* \to \widehat{\mathcal{O}_{\mathbb{K}}}^*/\widehat{\mathcal{O}}^* \to \mathcal{C}l(\mathcal{O}) \to \mathcal{C}l(\mathcal{O}_{\mathbb{K}}) \to 1. \tag{12.10}$$

Fourth example: any ray class field of an order
When $\mathcal{O} \subset \mathcal{O}_{\mathbb{K}}$ is an order, $\mathfrak{m}$ an invertible ideal of $\mathcal{O}$ and Σ a subset of real places of $\mathbb{K}$. The ray class group $\mathcal{C}l_{\mathfrak{m},\Sigma}(\mathcal{O})$ can be computed thanks to the following exact sequences

$$1 \to \mathcal{O}^*/\mathcal{O}_{\mathfrak{m}}^* \to (\mathcal{O}/\mathfrak{m})^* \times \{\pm 1\}^{\Sigma} \to \mathcal{C}l_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathcal{C}l(\mathcal{O}) \to 1 \tag{12.11}$$

where $\qquad \mathcal{O}_{\mathfrak{m}}^* := \{x \in \mathcal{O}^* \mid x \equiv 1 \bmod \mathfrak{m}\}.$

The exactness of (12.11) follows from (12.4), (12.5) and (12.10).

When the sign map $\mathcal{O}^* \to \{\pm 1\}^\Sigma$ is onto, the exact sequence (12.11) simplifies as

$$1 \to \mathcal{O}^*/\mathcal{O}^*_{\mathfrak{m},\Sigma} \to (\mathcal{O}/\mathfrak{m})^* \to \mathcal{C}l_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathcal{C}l(\mathcal{O}) \to 1 \qquad (12.12)$$

where $\qquad \mathcal{O}^*_{\mathfrak{m},\Sigma} := \{x \in \mathcal{O}^*_{\mathfrak{m}} \mid x_v > 0, \text{ for all } v \text{ in } \Sigma\}$.

Note that different extended ideals $\mathfrak{m}$ may give rise to the same subgroup $\mathcal{N}_{\mathfrak{m}}$ and hence to the same extension $\mathbb{K}_{\mathfrak{m}}$

Exercise 12.14. Assume that $\mathbb{K} = \mathbb{Q}$, $\mathcal{O} = \mathcal{O}_{\mathbb{K}} = \mathbb{Z}$ and $\mathfrak{m} = d\mathbb{Z}$ with $d \geqslant 2$.
a) Check that the quotient $C_{\mathbb{K}}/C^0_{\mathbb{K}}$ is isomorphic to the mutiplicative group $\widehat{\mathbb{Z}}^*$ of the ring $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/d\mathbb{Z}$.
b) Check that the extended ideal $(d\mathbb{Z}, \{\infty\})$ corresponds to the cyclotomic field $H_{d\mathbb{Z},+}(\mathbb{Z}) = \mathbb{Q}[e^{2i\pi/d}]$.
c) Check that the extended ideal $(d\mathbb{Z}, \varnothing)$ corresponds to the cyclotomic field $H_{d\mathbb{Z}}(\mathbb{Z}) = \mathbb{Q}[\cos(2\pi/d)]$.

Exercise 12.15. *a*) Check that $\mathbb{Q} = H_{\mathbb{Z},+}(\mathbb{Z}) = H_{2\mathbb{Z},+}(\mathbb{Z}) \neq H_{4\mathbb{Z},+}(\mathbb{Z})$.
b) Check that $\mathbb{Q} = H_{\mathbb{Z}}(\mathbb{Z}) = H_{2\mathbb{Z}}(\mathbb{Z}) = H_{4\mathbb{Z}}(\mathbb{Z}) \neq H_{8\mathbb{Z}}(\mathbb{Z})$.
c) How do Points *a*) and *b*) fit with (12.6)?
d) Prove using (12.6) that every finite abelian extension of $\mathbb{Q}$ is included in a cyclotomic field $\mathbb{Q}[\zeta_d]$ (Kronecker-Weber theorem).

Exercise 12.16. *a*) Let $\mathbb{K} = \mathbb{Q}[\sqrt{2}]$. Prove that the narrow Hilbert class field of $\mathbb{K}$ is $H_+(\mathcal{O}_{\mathbb{K}}) = \mathbb{K}$.
. *b*) Let $\mathbb{K} = \mathbb{Q}[\sqrt{3}]$. Prove that the narrow Hilbert class field of $\mathbb{K}$ is $H_+(\mathcal{O}_{\mathbb{K}}) = \mathbb{Q}[i, \sqrt{3}]$.

Exercise 12.17. Assume that $\mathcal{O} = \mathcal{O}_{\mathbb{K}}$. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ and Σ be a set of real places of $\mathbb{K}$. Check that $U_{\mathfrak{m},\Sigma}(\mathcal{O}_{\mathbb{K}}) = \prod_v U_v$ where

$$U_v = \begin{cases} \mathbb{R}^*_+ & \text{if } v \text{ is archimedean } v \in \Sigma, \\ \mathbb{K}^*_v & \text{if } v \text{ is archimedean } v \notin \Sigma, \\ 1+\mathfrak{m}_v & \text{if } v \text{ is non-archimedean, } \mathfrak{m}_v \neq \mathcal{O}_{\mathbb{K}_v}, \\ \mathcal{O}^*_{\mathbb{K}_v} & \text{if } v \text{ is non-archimedean, } \mathfrak{m}_v = \mathcal{O}_{\mathbb{K}_v}, \end{cases}$$

and where $\mathfrak{m}_v$ is the completion of $\mathfrak{m}$ in the ring $\mathcal{O}_{\mathbb{K}_v}$.
Indication: Note that, for almost all non-archimedean v one has $\mathfrak{m}_v = \mathcal{O}_{\mathbb{K}_v}$

and that by the chinese remainder theorem, one has a canonical isomorphism of rings

$$\mathcal{O}_{\mathbb{K}}/\mathfrak{m} \simeq \prod_{v} \mathcal{O}_{\mathbb{K}_v}/\mathfrak{m}_v \tag{12.13}$$

where the product is over all the finite places of $\mathbb{K}$.

Exercise 12.18. Let $\mathbb{K}$ be a real quadratic field.
a) Prove that the degree $[H_+(\mathcal{O}_{\mathbb{K}}) : H(\mathcal{O}_{\mathbb{K}})]$ is equal to 1 or 2.
b) Prove that it is 1 iff there exists $x \in \mathcal{O}_{\mathbb{K}}^*$ such that $N_{K/\mathbb{Q}}(x) = -1$.

13 The Artin map

In this lecture we give the precise definition of the Artin isomorphism which parametrizes the Galois group of the abelian extensions of number fields. This definition relies on the Artin reciprocity law which extends the Gauss quadratic reciprocity law.

We will then explain how Class Field Theory should describe the abelian extensions associated to HSIC, and how this Artin isomorphism should describe the Galois action on the correlations of a HSIC, according to [6] and [28].

13.1 Local Artin isomorphism

We come back to the notation of Section 12.2. Let K be a local field and L/K a finite abelian extension. We want to define precisely the Artin symbol

$$\mathrm{Art}_K = \mathrm{Art}_{L/K} : K^*/\mathcal{N}_L \to \mathrm{Gal}(L/K).$$

We recall that $\mathcal{N}_L := N_{L/K}(L^*)$ is the image in K^* of the norm map.

We first assume K archimedean. This case is easy since we have no choice.

When $K = \mathbb{R}$ and $\mathbb{L} = \mathbb{C}$, there is a unique way to identify two groups with 2 elements. For $a \in \mathbb{R}^*$, the image of a by the Artin map is given by the sign of a: one has $\mathrm{Art}_{\mathbb{R}}(a) \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and

$$\mathrm{Art}_{\mathbb{R}}(a) = 1 \Leftrightarrow a > 0.$$

When $\mathbb{K} = \mathbb{L} = \mathbb{R}$ or when $\mathbb{K} = \mathbb{L} = \mathbb{C}$ there is nothing to define.

Assume now that K is non-archimedean. We recall that $\mathcal{O}_K$ denotes its ring of integer, π a uniformizer, $\kappa = \mathcal{O}_K/\pi\mathcal{O}_K$ the residual field and $q = |\kappa|$. One has then $K^* \simeq \pi^{\mathbb{Z}} \times \mathcal{O}_K^*$.

We also recall that the Frobenius $F \in \mathrm{Gal}(L/K)$ of an unramified extension L/K is the automorphism such that, for all x in $\mathcal{O}_L$, one has $F(x) = x^q \bmod \pi\mathcal{O}_L$.

Theorem 13.1. *There are isomorphisms* $\mathrm{Art}_{L/K} : K^*/\mathcal{N}_L \to \mathrm{Gal}(L/K)$ *that are uniquely defined by the following three properties*
i) When L/K is unramified,

$$\mathrm{Art}_{L/K}(\pi) \ \text{ is the Frobenius of } L/K.$$

ii) When $L' \supset L \supset K$ *and* $a \in K^*$*, one has*

$$\mathrm{Art}_{L/K}(a) = \mathrm{Art}_{L'/K}(a)|_L.$$

iii) When $L \supset K \supset K'$ *and* $a \in K^*$ *then, setting* $a' = N_{K/K'}(a)$*, one has*

$$\mathrm{Art}_{L/K}(a) = \mathrm{Art}_{L/K'}(a').$$

Condition (ii) tells us that the maps $\mathrm{Art}_{L/K}$ do not depend on L. This is why we denote it by Art_K. This unique isomorphism $\mathrm{Art}_K = \mathrm{Art}_{L/K}$ is called the Artin symbol. It identifies the profinite completion of the topological group K^* with $\mathrm{Gal}(K^{ab}/K)$.

1. When the extension L/K is unramified and $a \in \mathcal{O}_K^*$, then $\mathrm{Art}_K(a)|_L = 1$. Indeed a belongs to $\mathcal{N}_L$. This explains why Condition i) does not depend on the choice of the uniformizer π.

3. For a, b in K^*, one defines the quadratic Hilbert symbol

$$(a,b)_K = \begin{cases} 1 & \text{if } x^2 - ay^2 - bz^2 = 0 \text{ has a non-zero solution in } K \\ -1 & \text{otherwise} \end{cases}$$

Hence one has

$$(a,b)_K = \tfrac{\mathrm{Art}_K(a)(\sqrt{b})}{\sqrt{b}} = \tfrac{\mathrm{Art}_K(b)(\sqrt{a})}{\sqrt{a}},$$

and this Hilbert symbol is a non-degenerate bilinear duality on K^*/K^{*2}.

Exercise 13.2. a) Compute K^*/K^{*2} for $K = \mathbb{Q}_p$ for p odd prime.
b) Compute the Hilbert symbol $(a,b)_K$ for $K = \mathbb{Q}_p$ with p odd prime.
c) Compute K^*/K^{*2} for $K = \mathbb{Q}_2$.
d) Compute the Hilbert symbol $(a,b)_K$ for $K = \mathbb{Q}_2$.

4. When $K = \mathbb{Q}_p$, one has $\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \simeq \widehat{\mathbb{Z}} \times \mathbb{Z}_p^*$.
In case $m \wedge p = 1$ and $a \in \mathbb{Z}_p^*$ one has

$$\mathrm{Art}_{\mathbb{Q}_p}(p)\zeta_m = \zeta_m^p \;\text{ and }\; \mathrm{Art}_{\mathbb{Q}_p}(a)\zeta_m = \zeta_m.$$

In case $m = p$, one has

$$\mathrm{Art}_{\mathbb{Q}_p}(p)\zeta_p = \zeta_p \;\text{ and, for } p \text{ odd, } \mathrm{Art}_{\mathbb{Q}_p}(a)\zeta_p = \zeta_p^{a^{-1}}.$$

Exercise 13.3. Let $K = \mathbb{Q}_2[\sqrt{5}]$ and $L = K[\sqrt{K^*}]$.
a) Check that $K^*/K^{*2} = \langle -1, 2, 1+\sqrt{5}\,, 2+\sqrt{5} \rangle \simeq \mathbb{F}_2^4$.
b) Check that $\mathcal{N}_L = K^{*2} = \langle 2, 1 + 8\mathcal{O}_K, 3+\sqrt{5} \rangle$.
c) Compute the Hilbert symbol on K^*/K^{*2}.
d) Compute the Artin isomorphism $\mathrm{Art}_{L/K}$.

13.2 Global Artin isomorphism

We come back to the notation of Section 12.5. Let $\mathbb{K}$ be a global field and $\mathbb{L}$ a finite abelian extension of $\mathbb{K}$. We can now give the precise definition of the Artin map. We recall that $C_{\mathbb{K}} := I_{\mathbb{K}}/\mathbb{K}^*$ denotes the idèles class group, and that $\mathcal{N}_{\mathbb{L}} := N_{L/K}(C_{\mathbb{L}})$ is the image in $C_{\mathbb{K}}$ of the norm map.

We just repeat the definition given in Theorem 12.11.c with the precise definition of the local Artin symbols in Section 13.1.

Theorem 13.4. *The local Artin symbols*

$$\mathrm{Art}_{\mathbb{K}_v} : \mathbb{K}_v^* \to \mathrm{Gal}(\mathbb{L}_w/\mathbb{K}_v) \hookrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{K})$$

induce an isomorphism

$$\begin{array}{rcl} \mathrm{Art}_{\mathbb{K}} : C_{\mathbb{K}}/\mathcal{N}_{\mathbb{L}} & \to & \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \\ x \bmod \mathcal{N}_{\mathbb{L}} & \mapsto & \mathrm{Art}_{\mathbb{K}}(x) := \prod_v \mathrm{Art}_{\mathbb{K}_v}(x_v), \end{array}$$

where $x \in C_{\mathbb{K}}$ is written as $x = (x_v) \bmod \mathbb{K}^*$.

The fact, which is implicit in this theorem, that one has the product formula

$$\prod_v \mathrm{Art}_{\mathbb{K}_v}(x_v) \;=\; 1\,, \quad \text{for all } x \text{ in } \mathbb{K}^*. \qquad (13.1)$$

is called the Artin reciprocity law. It is a far reaching extension of the quadratic reciprocity.

13.3 Quadratic and cubic reciprocity laws

For instance let us explain why Equality (13.1) implies the quadratic and the cubic reciprocity.

Application to the quadratic reciprocity

Let $\mathbb{K} = \mathbb{Q}$. For p, q in $\mathbb{N}$ distinct odd primes one recall the Legendre quadratic residue symbol

$$\left(\frac{p}{q}\right) \in \{\pm 1\} \text{ given by } \left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \bmod p.$$

One has then the quadratic reciprocity:

Corollary 13.5. $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$

Proof using (13.1). The quadratic Hilbert symbol, for a place ℓ of $\mathbb{Q}$, is

$$(p,q)_{\mathbb{Q}_\ell} = \mathrm{Art}_{\mathbb{Q}_\ell}(p)(\sqrt{q})/\sqrt{q} \in \{\pm 1\}$$

The Artin reciprocity tells us that these Hilbert symbols satisfy

$$(p,q)_{\mathbb{Q}_p}\,(p,q)_{\mathbb{Q}_q}\,(p,q)_{\mathbb{Q}_2}\,(p,q)_{\mathbb{Q}_\infty} = 1.$$

But one can compute directly each one of these symbols.

$$(p,q)_{\mathbb{Q}_p} = \left(\frac{q}{p}\right),\ (p,q)_{\mathbb{Q}_q} = \left(\frac{p}{q}\right),\ (p,q)_{\mathbb{Q}_2} = (-1)^{\frac{(p-1)(q-1)}{4}},\ (p,q)_{\mathbb{Q}_\infty} = 1.$$

This proves the quadratic duality. □

Application to the cubic reciprocity

Let $\mathbb{K} = \mathbb{Q}[\omega]$ with $\omega^2 + \omega + 1 = 0$. Recall that its ring of integers $\mathbb{Z}[\omega]$ is principal and that its group of units $\mathbb{Z}[\omega]^*$ has order 6. Therefore every ideal coprime to 3 has a unique generator which is equal to 1 mod 3.

For π, θ in $\mathbb{Z}[\omega]$ distinct irreducible elements that do not divide 3 and such that $\pi \equiv \theta \equiv 1$ mod 3, one defines the cubic residue symbol

$$\left(\frac{\pi}{\theta}\right)_3 \in \{1,\omega,\omega^2\} \text{ given by } \left(\frac{\pi}{\theta}\right)_3 = \pi^{\frac{N(\theta)-1}{3}} \bmod \theta,$$

where $N(\theta) = \#(\mathbb{Z}[\omega]/\theta\mathbb{Z}[\omega])$. Then, one has the cubic reciprocity law:

Corollary 13.6. $\left(\dfrac{\pi}{\theta}\right)_3 = \left(\dfrac{\theta}{\pi}\right)_3$

In particular, π is a cube modulo θ if and only if θ is a cube modulo π.

Proof using (13.1). We use the cubic Hilbert symbol for a place η of $\mathbb{K}$.

$$(\pi,\theta)_{\mathbb{K}_\eta} := \mathrm{Art}_{\mathbb{K}_\eta}(\pi)(\sqrt[3]{\theta})/\sqrt[3]{\theta} \in \{1,\omega,\omega^2\}$$

The Artin reciprocity tells us that these Hilbert symbols satisfy

$$(\pi,\theta)_{\mathbb{K}_\pi}\,(\pi,\theta)_{\mathbb{K}_\theta}\,(\pi,\theta)_{\mathbb{K}_{\omega-1}}\,(\pi,\theta)_{\mathbb{K}_\infty} = 1.$$

But one can compute directly each one of these symbols.

$$(\pi,\theta)_{\mathbb{K}_\pi} = \left(\frac{\theta}{\pi}\right)_3,\ (\pi,\theta)_{\mathbb{K}_\theta} = \left(\frac{\pi}{\theta}\right)_3,\ (\pi,\theta)_{\mathbb{K}_{\omega-1}} = 1,\ (\pi,\theta)_{\mathbb{K}_\infty} = 1.$$

This proves the cubic duality. □

13.4 HSIC and class field theory

In this section we explain, following [6] and [28], how class field theory for the real quadratic field $\mathbb{K} = \mathbb{Q}[\sqrt{\Delta_d}]$ with $\Delta_d = (d+1)(d-3)$ can be used to describe, conjecturally, the various fields of definition associated to the HSIC.

We come back to the notation of Lecture 10. Let $d \geqslant 4$. We set $d' = d$ when d is odd and $d' = 2d$ when d is even. Let $\zeta_d = e^{2i\pi/d}$ and $\eta_d = -e^{i\pi/d}$. Recall that the projective Heisenberg group PH_d is the subgroup of the projective unitary group $PU(d)$ isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$ generated by the two matrices $E = (\delta_{j,k+1})$ and $F = (\zeta_d^j \delta_{j,k})$. Recall that the group PEN_d is the normalizer of PH_d in the projective extended unitary group $PEU(d)$, and that the quotient group PEN_d/PH_d is isomorphic to $\mathrm{SL}^{\pm}(2, \mathbb{Z}/d\mathbb{Z})$. For $p = (p_1, p_2)$ in $(\mathbb{Z}/d'\mathbb{Z})^2$, the displacement matrix $D_p = \eta_d^{p_1 p_2} E^{p_1} F^{p_2} \in U(d)$ is well defined.

Let $P_0 = |v_0\rangle\langle v_0|$ be a fiducial projector, this is a rank one projector such that the correlations $u_p := tr(P_0 D_p)$ satisfy $|u_p|^2 = \frac{1}{d+1}$ for all in $(\mathbb{Z}/d'\mathbb{Z})^2$ with $p \not\equiv 0 \bmod d$.

We have defined the extensions

$$\mathbb{Q} \subset \mathbb{K} \subset \mathbb{E}_0 \subset \mathbb{E}_1 \subset \mathbb{E}.$$

of the field $\mathbb{K} = \mathbb{Q}[\sqrt{\Delta_d}]$. The extension $\mathbb{E}$ is generated by η_d and the entries of P_0. The extension $\mathbb{E}_1$ is $\mathbb{E}_1 = \sigma_0(\mathbb{E} \cap \mathbb{R})$ for some $\sigma_0 \in \mathrm{Gal}(\mathbb{C}/\mathbb{K})$ with $\sigma_0(\sqrt{\Delta_d}) = -\sqrt{\Delta_d}$. The extension $\mathbb{E}_0$ is the field of definition of the geometric class $[P_0]$ which is the PEN_d-orbit of P_0. Conjecturally, the field $\mathbb{E}$ is a Galois extension of $\mathbb{Q}$, and the group $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is abelian, and its action preserves the set of (hermitian) fiducial projectors $\mathcal{F}_{d,h}$. Conjecturally this set is finite.

Write $\Delta_d = f^2 D_0$ with D_0 fundamental discriminant so that f is the conductor of the ring $\mathbb{Z}[\varepsilon_d]$. Let f' be the divisor of f associated to the multiplet $[[P_0]]$ in Conjecture 10.9.

Conjecture 13.7. *a) The field $\mathbb{E}_0$ is the Hilbert class field of the ring $\mathcal{O}_{f'}$.*
b) The field $\mathbb{E}_1$ is the ray class field of the extended ideal $(d'\mathcal{O}_{f'}, \infty_1)$ of $\mathcal{O}_{f'}$.
c) The field $\mathbb{E}$ is the ray class field of its extended ideal $(d'\mathcal{O}_{f'}, \infty_1, \infty_2)$.

When $f' = 1$, Point $a)$ means that $\mathbb{E}_0$ is the maximal unramified abelian extension of $\mathbb{K}$.

When $f' = 1$, Point *b*) means that the finite index subgroup $\mathcal{N}_{\mathbb{E}_1} \subset C_{\mathbb{K}}$ of the idèles class group associated to $\mathbb{E}_1$ by (12.6) is the image in $C_{\mathbb{K}}$ of the subgroup of $I_{\mathbb{K}}$ generated by $1 + d'\mathcal{O}_{\mathbb{K}_v}$ at finite places v of $\mathbb{K}$ dividing d', by $\mathcal{O}^*_{\mathbb{K}_v}$ at all the other finite places, by $\mathbb{R}^*_+$ at the infinite place ∞_1, and by $\mathbb{R}^*$ at the other infinite place. And similarly for Point *c*).

One can check this conjecture for $d = 5$. Indeed in this case, one has $f = f' = 1$, $\mathbb{K} = \mathbb{Q}[\sqrt{3}]$ and $\mathbb{E}_1 = \mathbb{Q}[y]$ where the minimal polynomial of y over $\mathbb{Q}$ is the polynomial (12.3). We have seen that $\mathbb{E}_1$ is an abelian extension of $\mathbb{K}$ with Galois group $\mathbb{Z}/8\mathbb{Z}$. The discriminant of this polynomial (12.3) is equal to $2^8 5^7$, hence the field $\mathbb{E}_1 = \mathbb{Q}[y]$ is ramified over $\mathbb{K}$ only at the archimedean place $v = \infty_1$ and at the finite place $v = 5$. And we have already computed in Exercise 12.5 the image of the norm map for the completions at the place $v = 5$.

Corollary 13.8. *Assume Conjecture 13.7.*
a) The Galois group $\mathrm{Gal}(\mathbb{E}_0/\mathbb{K})$ *is isomorphic to the class group* $\mathcal{C}l(\mathcal{O}_{f'})$.
b) The Galois group $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ *is isomorphic to the quotient of the multiplicative group* $(\mathcal{O}_{f'}/d'\mathcal{O}_{f'})^*$ *by the subgroup image of* $\mathcal{O}^*_{f'}$.

13.5 HSIC and Artin isomorphism

In this section we explain how the Artin isomorphism for the abelian extension of the real quadratic field $\mathbb{K} = \mathbb{Q}[\sqrt{\Delta_d}]$ can be used to describe, conjecturally, the action of the absolute Galois group of $\mathbb{K}$ on the phases of a HSIC.

We come back to the notation of Section 13.4. And we assume Conjecture 13.7. In particular, we have two finite index subgroups corresponding to $\mathbb{E}_0$ and $\mathbb{E}_1$ in the idèles class group $C_{\mathbb{K}}$, the groups

$$\mathcal{N}_0 := \mathcal{N}(\mathcal{O}_{f'}) \text{ and } \mathcal{N}_1 := \mathcal{N}_{d'\mathcal{O}_{f'},\infty_1}(\mathcal{O}_{f'}),$$

so that the Artin map induces an isomorphism

$$Art : \mathcal{N}_0/\mathcal{N}_1 \xrightarrow{\sim} \mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0). \tag{13.2}$$

Note that there is a natural isomorphisms

$$(\mathcal{O}_{f'}/d'\mathcal{O}_{f'})^* \simeq \mathcal{N}_0/\mathcal{N}_1.$$

Let $z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$. This matrix satisfies $z^2 + z + 1 = 0$. Let $A_{d'} := (\mathbb{Z}/d'\mathbb{Z})[z] \subset \mathcal{M}(2, \mathbb{Z}/d'\mathbb{Z})$ be the Zauner ring and let $A_{d'}^*$ be the group of units, or invertible elements in the ring $A_{d'}$.

As in Conjecture 10.27, we assume $f' = f$. This assumption can probably be weakened. It insures the equalities $\mathcal{O}_f = \mathbb{Z}[\varepsilon_d] = \mathcal{O}_{f'}$ and hence rings isomorphisms

$$A_{d'} = \mathcal{O}_f/d'\mathcal{O}_f \simeq \mathcal{O}_{f'}/d'\mathcal{O}_{f'},$$

Therefore this gives an isomorphism

$$\psi : A_{d'}^* \simeq (\mathcal{O}_{f'}/d'\mathcal{O}_{f'})^* \simeq \mathcal{N}_0/\mathcal{N}_1. \tag{13.3}$$

We make the extra assumption 10.24 that $P_0 = |v_0 >< v_0|$ is strongly centred.

Conjecture 13.9. *For $a \in A_{d'}^*$, $p \in (\mathbb{Z}/d'\mathbb{Z})^2$, one has $u_{ap} = Art(\psi(a))(u_p)$.*

In conclusion the action of
the Galois group on the phases u_b
should be given by the Artin isomorphism.

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] D. M. Appleby. Symmetric informationally complete-positive operator valued measures and the extended Clifford group. *J. Math. Phys.*, 46:052107, 29, 2005.

[4] D. M. Appleby, H. Yadsan-Appleby, and G. Zauner. Galois automorphisms of a symmetric measurement. *Quantum Inf. Comput.*, 13:672–720, 2013.

[5] M. Appleby and I. Bengtsson. Simplified exact SICS. *J. Math. Phys.*, 60:062203, 14, 2019.

[6] M. Appleby, S. Flammia, G. McConnell, and J. Yard. SICs and algebraic number theory. *Found. Phys.*, 47:1042–1059, 2017.

[7] M. Appleby, S. Flammia, G. McConnell, and J. Yard. Generating ray class fields of real quadratic fields via complex equiangular lines. *Acta Arith.*, 192:211–233, 2020.

[8] A. Beauville. Theta functions, old and new. Surv. Mod. Math. 6, pages 99–132. Int. Press, 2013.

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

[10] Y. Benoist. Convolution and square in abelian groups II. hal-03744506 (2022).

[11] Y. Benoist. Fourier transform in cyclic groups. hal-04613351 (2024).

[12] Y. Benoist. On the rational symplectic group. Progress in Math. 357 (2025) p.241-250.

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

[14] C. Birkenhake and H. Lange. *Complex abelian varieties.* Grundlehren Math. 302. Springer, 2004.

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

[16] 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.

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

[18] O. Debarre. *Tores et variétés abéliennes complexes.* Cours Spécialisés. SMF, 1999.

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

[20] C. Fuchs, M. Hoang, and B. Stacey. The sic question: History and state of play. arXiv:1703.07901 (2017).

[21] P. Griffiths and J. Harris. *Principles of algebraic geometry.* Wiley, 1978.

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

[23] S. Hoggar. 64 lines from a quaternionic polytope. *Geom. Dedicata*, 69:287–289, 1998.

[24] L. Hughston and S. Salamon. Surveying points in the complex projective plane. *Adv. Math.*, 286:1017–1052, 2016.

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

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

[27] G. Kopp and J. Lagarias. Ray class groups and ray class fields for orders of number fields. arXiv:2212.09177.

[28] G. Kopp and J. Lagarias. Sicpovms and orders of real quadratic fields. arXiv:2407.08048.

[29] G. S. Kopp. Indefinite zeta functions. *Res. Math. Sci.*, 8:No. 17, 34, 2021.

[30] G. S. Kopp. SIC-POVMs and the Stark conjectures. *Int. Math. Res. Not. IMRN*, (18):13812–13838, 2021.

[31] G. S. Kopp. A Kronecker limit formula for indefinite zeta functions. *Res. Math. Sci.*, 10:No. 24, 21, 2023.

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

[33] S. Lang. *Algebra.* GTM 211. Springer, 2002.

[34] P. Lemmens and J. Seidel. Equiangular lines. *J. Algebra*, 24:494–512, 1973.

[35] D. Mumford. *Tata lectures on theta. I.* PM 28. Birkhäuser, 1983.

[36] M. Neuhauser. An explicit construction of the metaplectic representation over a finite field. *J. Lie Theory*, 12:15–30, 2002.

[37] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45:2171–2180, 2004.

[38] A. Scott. Sics: extending the list of solutions. arXiv:1703.03993 (2017).

[39] A. J. Scott and M. Grassl. Sic-povms: a new computer study. *J. Math. Phys.*, 51:042203, 16, 2010.

[40] G. Shimura. Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan*, 15:33–65, 1963.

[41] G. Shimura. On modular correspondences for $Sp(n, Z)$ and their congruence relations. *Proc. Nat. Acad. Sci. U.S.A.*, 49:824–828, 1963.

[42] P. Stevenhagen. Hilbert's 12th problem, complex multiplication and Shimura reciprocity. In *Class field theory*, Adv. Stud. Pure Math., pages 161–176. 2001.

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

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

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

[46] S. F. D. Waldron. *An introduction to finite tight frames.* Applied and Numerical Harmonic Analysis. Birkhäuser, 2018.

[47] G. Zauner. Quantum designs: foundations of a noncommutative design theory. *Int. J. Quantum Inf.*, 9:445–507, 2011.