Convolution and square in abelian groups

Yves Benoist

CNRS - Paris-Saclay University

Tokyo, September 2022

1. Critical values

Let G be a finite abelian group of odd order d.

Aim Describe $f : G \to \mathbb{C}$ non-zero and $\lambda \in \mathbb{C}$ such that

$$\sum_{y\in G} f(x+y)f(x-y) \;=\; \lambda\, f(x)^2.$$

λ is a critical value on G,
f is a λ-critical function on G.

Example: $G = \mathbb{Z}/d\mathbb{Z}$: λ is called d-critical

Proposition 1 Let λ be a critical value on G. Then
⋆ $|\lambda| \le d$,
⋆ d/λ is also a critical value on G,
⋆ the Galois conjugate of λ too,
⋆ $(\lambda-1)/2$ is an algebraic integer.

Given G there are only finitely many λ.
Given G and λ there are often infinitely many f.

When $G = \mathbb{R}$?

2. Examples

λ critical on G : $\sum_{y\in G} f(x+y)f(x-y) = \lambda\, f(x)^2$.

List of critical values for $d = 11$

up to Galois conjugation,
⋆ $\lambda = 1$,
⋆ $\lambda = 11$,
⋆ $\lambda = 4+\sqrt{5}$,
⋆ $\lambda = i\sqrt{11}$,
⋆ $\lambda = 2+i\sqrt{7}$ and $2\sqrt{2}+i\sqrt{3}$,
⋆ $\pm\lambda = 1+\sqrt{5}+i\sqrt{5-2\sqrt{5}}$.

The aim of this talk is to explain this list! The proof will use
⋆ abelian varieties with complex multiplication,
⋆ theta functions on torsion points and
⋆ modular functions on the Siegel upper half space.

Proposition 2 $d = a+b$ positive integers.
When $a \equiv \frac{(d+1)^2}{4} \bmod 4$, then
$\lambda = \sqrt{a}+i\sqrt{b}$ is d-critical.

This elementary statement does not have an elementary proof!

Proposition 3 $d = a+b+c$ positive integers with $b^2 > 4ac$.
(i) When $a \equiv b \equiv c \equiv 1 \bmod 4$, then
$\lambda = \sqrt{a}+\sqrt{c}+i\sqrt{b-2\sqrt{ac}}$ is d-critical.
(ii) When $a \equiv b \equiv c \equiv 3 \bmod 4$, then
$\lambda = i\sqrt{a}+i\sqrt{c}+\sqrt{b-2\sqrt{ac}}$ is d-critical.

These elementary statements do not have elementary proofs either!

3. Abelian varieties

Let (A,ω) be a ppav (principally polarized abelian variety):
⋆ $A = \mathbb{C}^n/\Lambda$ is a complex torus, $\Lambda \subset \mathbb{C}^n$ is a lattice.
⋆ $\omega = \mathrm{Im}(H)$ where H is a positive hermitian form on $\mathbb{C}^n$
with $\omega(\Lambda,\Lambda) \subset \mathbb{Z}$ and $\det_\Lambda(\omega) = 1$.

Let $\mathrm{End}_{\mathbb{Q}}(A) := \{\nu \in \mathrm{End}(\mathbb{C}^n) \mid \nu(\Lambda_{\mathbb{Q}}) \subset \Lambda_{\mathbb{Q}}\}$.
$h_\nu := \nu|_{\Lambda_{\mathbb{Q}}}$ is called the holonomy of ν.

ν is unitary for $H \iff h_\nu$ is symplectic for ω.

Theorem Let $\nu \in \mathrm{End}_{\mathbb{Q}}(A)$ be unitary satisfying $(\star)$
Let $G_\nu := \Lambda/(\Lambda \cap \nu\Lambda)$ and $d_\nu := |G_\nu|$. Then
$\lambda = \kappa\, d_\nu^{1/2} \det_{\mathbb{C}}(\nu)^{1/2}$ is critical on G_ν for some $\kappa^4 = 1$.

$(\star)$: Writing $h_\nu = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ in a symplectic basis of Λ, one has
$h_\nu \equiv 1 \bmod 2$ and $\beta_{ii} \equiv \gamma_{ii} \equiv 0 \bmod 4$, for all $i \le n$.

Theorem $\Longrightarrow$ Proposition 2. $\lambda = \sqrt{a}+i\sqrt{b}$ is d-critical.
Chose $n = 1$, $\nu = \frac{\sqrt{a}+i\sqrt{b}}{\sqrt{a}-i\sqrt{b}}$, $\Lambda = \mathbb{Z}i\sqrt{ab} \oplus \mathbb{Z} \subset \mathbb{C}$.

Theorem $\Longrightarrow$ Proposition 3.(i). $\lambda = \sqrt{a}+\sqrt{c}+i\sqrt{b-2\sqrt{ac}}$ is d-critical.
Choose $n = 2$, $\nu = \frac{1+t_+}{1-t_+}$ with $t_\pm = \sqrt{\frac{-b\pm\delta}{2a}}$, $\delta = \sqrt{b^2-4ac}$,
$\Lambda = \mathbb{Z} \oplus \mathbb{Z}\frac{b+\delta}{2} \oplus \mathbb{Z}\frac{2+(b-\delta)t}{4} \oplus \mathbb{Z}\frac{b+\delta-2\delta t_+}{4} \subset \mathbb{C}^2$.

4. CM number fields

Let K be a CM-number field = totally imaginary quadratic extension of a totally real number field
$2n = [K:\mathbb{Q}]$,
Φ a CM-type
so that $\mathrm{Hom}(K,\mathbb{C}) = \Phi \cup \overline{\Phi}$.

For $\mu \in K$, let $N_\Phi(\mu)$ be the reflex norm of μ
so that $N_{K/\mathbb{Q}}(\mu) = |N_\Phi(\mu)|^2$ is the norm of μ.

Corollary
If $K/(K\cap\mathbb{R})$ is ramified or $K = \mathbb{Q}[e^{2i\pi/\ell}]$ $(\star\star)$.
Let $s \in \mathcal{O}_K$ and $\mu = 1+s-\overline{s}$ with $d := N_{K/\mathbb{Q}}(\mu)$ odd.
Then $\lambda := N_\Phi(\mu)$ or $-\lambda$ is critical on $\mathcal{O}_K/\mu\mathcal{O}_K$.

Example with $s = e^{2i\pi/\ell}$ where $\ell \ge 5$ is prime.
Then $\lambda := \prod_{k<\ell/2} (1+2i\sin(k\pi/\ell))$ or $-\lambda$ is d-critical,
with $d = |\lambda|^2 = L_\ell = F_{\ell-1}+F_{\ell+1}$ = Lucas number.

Remark $(\star\star)$ implies the existence of an ideal $\mathfrak{m} \subset \mathcal{O}_K$
such that $A = \mathbb{C}^n/\Phi(\mathfrak{m})$ is a ppav, by Shimura-Taniyama.

Theorem $\Longrightarrow$ Corollary. Choose $\Lambda = \Phi(\mathfrak{m})$, $\nu = \mu/\overline{\mu}$
so that $G_\nu \simeq \mathcal{O}_K/\mu\mathcal{O}_K$ and
$d_\nu \det_{\mathbb{C}}(\nu) = N_{K/\mathbb{Q}}(\mu) N_\Phi(\nu) = N_\Phi(\mu)^2$.

5. Theta functions **Proof of Theorem.**

Theorem : Let $\nu \in \mathrm{End}_{\mathbb{Q}}(A)$ unitary satisfying $(\star)$.
Set $G_\nu := \Lambda/(\Lambda\cap\nu\Lambda)$ and $d_\nu := |G_\nu|$. Then
$\lambda = \kappa\, d_\nu^{1/2} \det_{\mathbb{C}}(\nu)^{1/2}$ is critical on G_ν, for some $\kappa^4 = 1$.

One has $A = \mathbb{C}^n/(\tau\mathbb{Z}^n \oplus \mathbb{Z}^n)$, where $\tau \in \mathcal{H}_n$.

$\mathcal{H}_n = \{\tau \in \mathcal{M}(n,\mathbb{C})$ symmetric with $\mathrm{Im}(\tau) > 0\}$,
$\simeq \mathrm{Sp}(n,\mathbb{R})/U(n)$.

For $\sigma = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{Sp}(n,\mathbb{R})$, one has $\sigma.\tau = (\alpha\tau+\beta)(\gamma\tau+\delta)^{-1}$.

For $z \in \mathbb{C}^n$, set $\theta_\tau(z) := \sum_{m\in\mathbb{Z}^n} e^{i\pi\, {}^t m\tau m} e^{2i\pi\, {}^t m z}$.

Set $\Gamma^2 = \{\sigma \in \mathrm{Sp}(n,\mathbb{Z}) \mid \sigma \equiv 1 \bmod 2\}$,
$\Gamma^{\theta,2} = \{\sigma \in \Gamma^2 \mid \beta_{ii} \equiv \gamma_{ii} \equiv 0 \bmod 4$ for all $i \le n\}$.
= Theta subgroup of level 2 = Igusa subgroup.

Key lemma If there exists $\sigma \in \Gamma^{\theta,2}$ and $\mathrm{d} \in \mathcal{M}(n,\mathbb{Z})$
with $\det(\mathrm{d})$ odd and $\sigma.\tau = {}^t\mathrm{d}\tau\mathrm{d}$. Set $G := \mathrm{d}^{-1}\mathbb{Z}^n/\mathbb{Z}^n$.
Then, for all z in $\mathbb{C}^n$, the function

$$G \to \mathbb{C};\; w \mapsto \theta_\tau(z+w)$$

is λ-critical on G with

$$\lambda = \kappa_\sigma \det_{\mathbb{C}}(\gamma\overline{\tau}+\delta)^{-1/2}, \quad \text{for some } \kappa_\sigma^8 = 1.$$

Remark. The existence of such τ, σ and d follows from the existence of ν by writing
$h_\nu = \sigma_1 \begin{pmatrix}{}^t\mathrm{d} & 0\\ 0 & \mathrm{d}^{-1}\end{pmatrix} \sigma_2$ with $\sigma_j \in \mathrm{Sp}(n,\mathbb{Z})$ and $\mathrm{d} = \mathrm{diag}(d_1,\dots,d_n)$.

Proof of Key Lemma There are three key tools.

Key Lemma : $\sum_{w\in G} \theta_\tau(z+w)\theta_\tau(z-w) = \lambda\,\theta_\tau(z)^2$ for all $z \in \mathbb{C}^n$.

A. Addition formula. For z, w in $\mathbb{C}^n$, one has

$$\theta_\tau(z+w)\,\theta_\tau(z-w) = \sum_{\xi\in\mathbb{Z}^n/2\mathbb{Z}^n} \theta_{[\xi]}(w,\tau)\,\theta_{[\xi]}(z,\tau)$$

where $\theta_{[\xi]}(z,\tau) = \sum_{m\in\xi} e^{i\pi\, {}^t m \frac{\tau}{2} m}\, e^{2i\pi\, {}^t m z}$.

B. Isogeny formula. For $\xi \in \mathbb{Z}^n/2\mathbb{Z}^n$, one has

$$\frac{1}{|G|}\sum_{w\in G} \theta_{[\xi]}(w,\tau) \;=\; \theta_{[\xi]}(0, {}^t\mathrm{d}\tau\mathrm{d}).$$

C. Transformation formula. For $\sigma \in \Gamma^{\theta,2}$,
the following ratios do not depend on $\xi \in \mathbb{Z}^n/2\mathbb{Z}^n$,

$$j(\sigma,\tau) = \frac{\theta_{[\xi]}(0,\sigma.\tau)}{\theta_{[\xi]}(0,\tau)}$$

and $j(\sigma,\tau) = \kappa_\sigma \det_{\mathbb{C}}(\gamma\tau+\delta)^{1/2}$ with $\kappa_\sigma^8 = 1$.

Remark. This means that the functions $\tau \mapsto \theta_{[\xi]}(0,\tau)$ are modular functions
with same multipliers on the arithmetic quotient $\Gamma^{\theta,2}\backslash\mathcal{H}_n$.

6. Open questions

Q1. If λ is d-critical with d prime and $\lambda \ne 1, d$,
then λ and d/λ are Galois conjugate ?

Remark. If d_1 divides d and λ_1 is d_1-critical, then λ_1 is also d-critical.

Q2. If $d = a+b$ with $a \equiv \frac{(d+1)^2}{4} \bmod 4$ and $d \not\equiv 2 \bmod 3$.
then $\lambda := -\sqrt{a}-i\sqrt{b}$ is also d-critical ?

Remark. For $d = 5$, the value $\lambda := -1-2i$ is not d-critical.
For $d = 11$, the value $\lambda := -2-i\sqrt{7}$ is not d-critical.

FINAL CHALLENGE
For Proposition 2,
find a proof that does
not use elliptic curves.