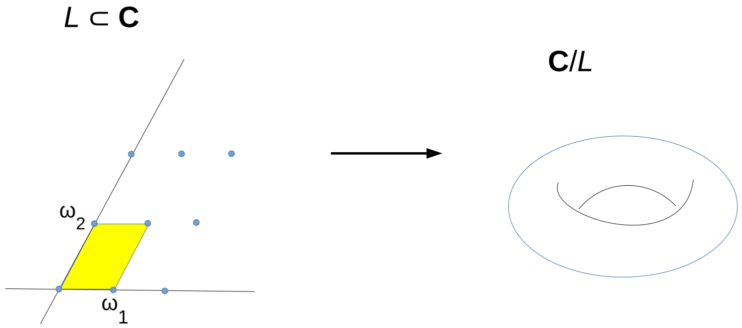
Meromorphic functions and projective embeddings of abelian varieties

Kamal Khuri-Makdisi
American University of Beirut

Mathematics in Lebanon and Beyond
January 2024

1. Complex tori

- A lattice $L \subset \mathbf{C}^g$ is a subgroup $L = \mathbf{Z}\omega_1 \oplus \cdots \oplus \mathbf{Z}\omega_{2g} \cong \mathbf{Z}^{2g}$, where the ω_i are linearly independent over $\mathbf{R}$.
- We study complex tori $X = \mathbf{C}^g/L$.
- Here is a picture when $g = 1$ and $L = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$.



2. Meromorphic functions on a complex torus

•When $g = 1$ and $L = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$. there are many meromorphic functions on $\mathbf{C}/L$ — these are the same as meromorphic functions on $\mathbf{C}$ that are periodic with respect to L.

•For example, for $d \geq 3$, the function $f_d(z) = \sum_{\ell \in L}(z - \ell)^{-d}$ converges and is periodic, with a pole of order d at each lattice point. This corresponds to a meromorphic function f_d on $\mathbf{C}/L$ with a pole at 0.

•A slight modification produces a convergent f_2, also known as the Weierstrass $\wp$ function. Then $\wp' = -2f_3$; similarly for all f_d.

•Fact: all meromorphic functions on $\mathbf{C}/L$ are rational functions of $\wp$ and $\wp'$. There is also a relation $(\wp')^2 = 4\wp^3 + \alpha\wp + \beta$, with constants $\alpha, \beta \in \mathbf{C}$ (which are determined by L).

•However, when $g \geq 2$, for "most" $L \subset \mathbf{C}^g$ there are NO nonconstant meromorphic functions on $\mathbf{C}^g/L$. Only for special L do "enough" meromorphic functions exist.

•The essential reason: poles of a meromorphic function occur on analytic subsets of $\mathbf{C}^g/L$ of dimension $g - 1$. For example, why should there be any complex curves on $\mathbf{C}^2/L$?

3. Motivating line bundles

•A different approach to finding meromorphic functions $f : \mathbf{C}^g \to \mathbf{C}$ that are periodic with respect to L is to realize them as quotients $f(z) = s(z)/t(z)$, where s and t are holomorphic quasi-periodic functions, that satisfy

$$s(z + \ell) = a_\ell(z)s(z), \quad t(z + \ell) = a_\ell(z)t(z), \quad \forall \ell \in L.$$

Here the $a_\ell(z)$ are a family of holomorphic functions, that need to satisfy the cocycle condition $a_{\ell+\ell'}(z) = a_\ell(z + \ell')a_{\ell'}(z)$.

•Since $a_0(z) = 1$, the $a_\ell(z)$ are never zero. Replacing both $s(z)$ and $t(z)$ by $g(z)s(z)$ and $g(z)t(z)$ does not change f, but changes the a_ℓ by a coboundary (in an appropriate cohomology group).

•In fancy language: A choice of family $a_\ell(z)$ (up to coboundary) describes a holomorphic line bundle $\mathcal{L}$ on $\mathbf{C}^g/L$, and then the functions $s(z), t(z)$ are sections of $\mathcal{L}$. For a given $p \in \mathbf{C}^g/L$ represented by $z \in \mathbf{C}^g$, the values $s(p), t(p)$ belong to the fiber $\mathcal{L}_p$, which is a one-dimensional complex vector space that varies nicely ("holomorphically") with p. The ratio $s(p)/t(p)$, when $t(p) \neq 0$, is a well-defined complex number.

4. Theta functions

•**For those unfamiliar with line bundles:** This talk will mainly express things in terms of a_ℓ and the relation $s(z+\ell) = a_\ell(z)s(z)$.
•Fact: up to coboundaries, the family a_ℓ for our complex torus can be of a very specific form, exponentials of linear functions. So $a_\ell(z) = e(A_\ell \cdot z + B_\ell)$, where $A_\ell \in \mathbf{C}^g$ and $B_\ell \in \mathbf{C}$. Here $e(c) = \exp(2\pi i c)$, and we view elements of $\mathbf{C}^g$ as column vectors; then $v \cdot w = {}^t vw$, the usual (nonhermitian) bilinear form.
•Fact: there are "enough" meromorphic functions on $\mathbf{C}^g/L$ if and only if up to changing coordinates on $\mathbf{C}^g$, the lattice L is equal to (in reality, contains) the lattice $\mathbf{Z}^g \oplus \Omega\mathbf{Z}^g$, where $\Omega \in M_g(\mathbf{C})$ is a symmetric complex matrix with Im Ω positive definite.
•In the above situation, for each $k \geq 1$ we can consider the distinguished family a_ℓ^k that corresponds to functions s that satisfy

$$s(z+n) = s(z), \quad \forall n \in \mathbf{Z}^g,$$

$$s(z+\Omega m) = e(-km \cdot \Omega m/2 - km \cdot z)s(z), \quad \forall m \in \mathbf{Z}^g.$$

•Functions s as above are called theta functions of weight k; the space of such theta functions has dimension k^g.

5. Meromorphic functions and projective embeddings

- The space of weight k theta functions:
  $s(z+n) = s(z), \quad s(z+\Omega m) = e(-km\cdot\Omega m/2 - km\cdot z)s(z).$
- A basis for the space of weight k theta functions is
  $$\theta_{k,c} = \sum_{n\equiv c \bmod k\mathbf{Z}^g} e(n\cdot\Omega n/2k + n\cdot z)), \quad \text{for } c\in \mathbf{Z}^g/k\mathbf{Z}^g.$$
- Fact: every meromorphic function on $\mathbf{C}^g/L$ is a ratio of two theta functions for all large k (depending on the function in question).
- For $k\geq 3$, the space of theta functions gives algebraic coordinates on $\mathbf{C}^g/L$, more precisely an embedding of $\mathbf{C}^g/L$ into the projective space $\mathbf{P}^{k^g-1}$, given by sending z to the projective point $[\theta_{k,0}(z):\cdots:\theta_{k,c}(z):\cdots]\in\mathbf{P}^{k^g-1}$.
- Here $\mathbf{P}^N$ is the quotient of $\mathbf{C}^{N+1}-\{0\}$ by the equivalence relation $(x_0,\cdots,x_N)\sim(\lambda x_0,\cdots,\lambda x_N)$ for $\lambda\in\mathbf{C}^*$. The equivalence classes are written $[x_0:\cdots:x_N]$.
- When $g=1$ and $k=3$, we have a 3-dimensional space of theta functions, and there exists a basis $\{s_0,s_1,s_2\}$ giving essentially $z\mapsto[x_0:x_1:x_2]=[s_0(z):s_1(z):s_2(z)]=[1:\wp(z):\wp'(z)]$ with equation $x_2^2x_0 = 4x_1^3+\alpha x_1x_0^2+\beta x_0^3 \iff (\wp')^2 = 4\wp^3+\alpha\wp+\beta.$

6. More on maps to projective space

- For $k = 3$, the map given by theta functions of weight k embeds $\mathbf{C}^g/L$ to projective space as a projective variety given by polynomials of degrees 2 and 3.
- For $k \geq 4$, we only need polynomials of degree 2.
- When $g = 1$, the weight 4 embedding amounts to two degree 2 polynomial equations on $\mathbf{P}^3$ (i.e., in 4 variables). The weight 3 embedding is the usual cubic model of an elliptic curve in $\mathbf{P}^2$.
- When $g = 2$, the weight 4 embedding is "cleaner" and more symmetric than the weight 3 embedding. However it requires 72 degree 2 equations on $\mathbf{P}^{15}$ (i.e., in 16 variables).
- The theta functions of weight 2 do not embed the complex torus, but they do map the quotient space $(\mathbf{C}^g/L)/[\pm 1]$ to projective space. Thus quotient space is called the Kummer variety.
- When $g = 1$, the weight 2 theta functions give the map from an elliptic curve to $\mathbf{P}^1$ given by $\wp$ (i.e., the x-coordinate on the cubic).
- When $g = 2$, the weight 2 theta functions usually embed the Kummer variety as a surface in $\mathbf{P}^3$ given by a single equation in degree 4.

7. The Edwards model

- We search for other usable algebraic models of $\mathbf{C}^g/L$. One can combine different maps from theta functions (and their translates) to embed $\mathbf{C}^g/L$ into a product of projective spaces.
- Specifically, consider the Kummer map $\kappa : \mathbf{C}^g/L \to \mathbf{P}^{2^g-1}$ given by the weight 2 theta functions, and suppose we are in the usual situation where $\kappa(p) = \kappa(q) \iff p = \pm q$.
- Fix a point $p_0 \in \mathbf{C}^g/L$ with $2p_0 \neq 0$. Then the map

  $p \mapsto (\kappa(p), \kappa(p + p_0)) \in \mathbf{P}^{2^g-1} \times \mathbf{P}^{2^g-1}$

  is an embedding. We will primarily use a point p_0 of order 4.
- When $g = 1$, this embeds an elliptic curve into $\mathbf{P}^1 \times \mathbf{P}^1$ in what is called the Edwards model. It is particularly convenient for computations over finite fields, used in cryptographic applications and elsewhere. The (inhomogeneous) equation of the Edwards model can be written as $Y^2 + U^2 = 1 + dU^2Y^2$; if d is not a square over the ground field K, this curve does not have rational points at infinity, so one can work entirely over K^2 without needing to pass to the projective plane over K. The group law operations also look more uniform than in the usual cubic model.

8. Generalization to $g = 2$

- This is joint work with E. V. Flynn. See arxiv:2211.01450.
- The Kummer map $\kappa : \mathbf{C}^2/L \to \mathbf{P}^3$ gives rise (usually) to an embedding in $\mathbf{P}^3 \times \mathbf{P}^3$, so using 8 variables (or just 6 if we can avoid points at infinity).
- The resulting image is described by explicit equations of the following types:
  - One equation in each bidegree $(4, 0)$ and $(0, 4)$ (the Kummer quartics in each $\mathbf{P}^3$),
  - Four equations in each bidegree $(2, 1)$ and $(1, 2)$,
  - Five more elements of bidegree $(2, 2)$.
- The total number of equations is thus 15. This is much more tractable than previous models with 72 equations in 16 variables.
- The model works over any field that is not of characteristic 2, for the Jacobian of a curve of genus 2 with certain rationality conditions and a Richelot isogeny to the Jacobian of another curve of genus 2.
- We give a nice version of the group law and can give cases where there are no "points at infinity".

9. Thank you for your attention!

10.

11.