

Report on the article

“ALGEBRAIC MAPS CONSTANT ON ISOMORPHISM CLASSES OF UNPOLARIZED ABELIAN VARIETIES ARE CONSTANT”

The article investigates the difference between isomorphism of polarized abelian varieties and isomorphism of abelian varieties (without polarization); namely, over the set of isomorphism classes of principally polarized abelian varieties (of fixed dimension over an algebraically closed field), when one forgets the polarization, “how much more extra isomorphisms” between the elements can appear? This question arose naturally in the construction of moduli space of abelian varieties, and the authors re-visits this question due to its connection to cryptography.

The article gives a satisfactory answer of this question in many slightly different settings. For example, Theorem 1.2, the most beautiful theorem of the article in my opinion, asserts that for the coarse moduli scheme A_g (with $g > 1$) over an algebraically closed field k , the equivalence relation $W_g \subset A_g(k) \times A_g(k)$ representing isomorphisms of abelian varieties (forgetting the polarization), is *Zariski dense* in $A_g \times A_g$. The proof of the theorem is by constructing sufficiently many extra isomorphisms among products of elliptic curves with complex multiplication.

The results are fundamental in algebraic geometry, and I am surprised that such important results were not proved before. My final opinion is to recommend the article for publication in ANT.

The mathematics of the paper is carefully written. The following are some minor suggestions or questions.

- p. 1, first paragraph, when \mathcal{A}_g is introduced, emphasize that it is the coarse moduli scheme.
- p. 1, Theorem 1.1, the setting over R . This is actually a problem in the statements of many theorems of the paper. You state the result over a domain R , but the proof is reduced to algebraically closed fields immediately by the second paragraph after the theorem, which means that the result over R is not really stronger. The statement over R in Theorem 1.1 is very sloppy; for example, “ (A_1, λ_1) and (A_2, λ_2) are in the domain of definition of f ” needs explanation. This sentence is also in Theorem 1.3.

My suggestion is to state the theorem over an algebraically closed field k , and do the same changes to all other similar theorems (Theorem 1.2, Theorem 1.3, etc). Then Remark 1.11 does the job of generalization. If I understand correctly, Proposition 4.8 is the only one where a general base ring R is necessary.

- p. 3, line 14, “principal polarization λ on B ”. The paper never checks that it is a principle polarization, though it is just a line of calculation of the degree. For its importance and for the readers, you may add it in the statement of Lemma 2.10, and refer to the lemma here.
- p. 3, line 16, the definition of ψ_A . It will be very helpful for the readers if you mention the complex results of Proposition 4.7 here. Moreover, mention the result of Lemma 2.10 here that B (forgetting the polarization) is isomorphic to a product of elliptic curves.
- p. 8, line 11, “ensures that there is an elliptic curve”. The existence needs more explanation. For example, CM elliptic curves or its reduction.
- p. 11, Lemma 4.6, the map $\tau \mapsto \tau A$ needs more explanation. How is τA an element of \mathbb{H}_g ?
- p. 13, Proposition 4.8. Give definitions or references for R -valued Siegel modular form and also q -expansion of modular forms over R . Moreover, for “ ℓ is a prime number not equal to the characteristic of the base ring R ”, do you mean “not equal to the characteristic of the residue field of any prime ideal of the base ring R ”?
- p. 13, last paragraph. For the proof of Theorem 1.10, if the base ring is just \mathbb{C} , do we have a simpler (analytic) proof in terms of the interpretation in Proposition 4.7?