ARTICLE IN PRESS YJNTH:6012

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Fields generated by sums and products of singular moduli

Bernadette Faye[a,*], Antonin Riffaut[b]

[a] *Université Cheikh Anta Diop de Dakar, BP: 5005, Dakar Fann, Senegal*
[b] *Institut de Mathématiques de Bordeaux, Université de Bordeaux, 351, cours de la Libération, 33 405 Talence cedex, France*

A R T I C L E I N F O

Article history:
Received 14 January 2018
Received in revised form 5 March 2018
Accepted 6 March 2018
Available online xxxx
Communicated by L. Smajlovic

Keywords:
Singular moduli
Complex multiplication
André-Oort
j-Invariant

A B S T R A C T

We show that the field $\mathbb{Q}(x, y)$, generated by two singular moduli x and y, is generated by their sum $x + y$, unless x and y are conjugate over $\mathbb{Q}$, in which case $x + y$ generates a subfield of degree at most 2. We obtain a similar result for the product of two singular moduli.

Contents

* Corresponding author.
E-mail address: bernadette@aims-senegal.org (B. Faye).

https://doi.org/10.1016/j.jnt.2018.03.015

Please cite this article in press as: B. Faye, A. Riffaut, Fields generated by sums and products of singular moduli, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.03.015

1. Introduction

A *singular modulus* is the j-invariant of an elliptic curve with complex multiplication. Given a singular modulus x we denote by Δ_x the discriminant of the associated imaginary quadratic order. We denote by $h(\Delta)$ the class number of the imaginary quadratic order of discriminant Δ. Recall that two singular moduli x and y are conjugate over $\mathbb{Q}$ if and only if $\Delta_x = \Delta_y$, and that all singular moduli of a given discriminant Δ form a full Galois orbit over $\mathbb{Q}$. In particular, $[\mathbb{Q}(x) : \mathbb{Q}] = h(\Delta_x)$. For all details, see, for instance, [7, §7 and §11]

Starting from the ground-breaking article of André [3] equations involving singular moduli were studied by many authors, see [2,5,9] for a historical account and further references. In particular, Kühne [8] proved that equation $x + y = 1$ has no solutions in singular moduli x and y, and Bilu et al. [6] proved the same for the equation $xy = 1$. These results where generalized in [2] and [5].

Theorem 1.1. ([2,5]) *Let x and y be singular moduli such that $x + y \in \mathbb{Q}$ or $xy \in \mathbb{Q}^\times$. Then either $h(\Delta_x) = h(\Delta_y) = 1$ or $\Delta_x = \Delta_y$ and $h(\Delta_x) = h(\Delta_y) = 2$.*

Here the statement about $x + y$ is (a special case of) Theorem 1.2 from [2], and the statement about xy is Theorem 1.1 from [5].

Note that lists of all imaginary quadratic discriminants Δ with $h(\Delta) \le 2$ are widely available, so Theorem 1.1 is fully explicit.

We may mention also a work of Bilu, Luca and Masser [4], who proved that all but finitely many straight lines $Ax + By = C$ with $A, B \in \bar{\mathbb{Q}}^\times$ and $C \in \bar{\mathbb{Q}}$ have no more than two CM-points (points whose both coordinates are singular moduli). This result is, however, non-effective, because it relies on a non-effective theorem of Pila.

In view of Theorem 1.1 one may ask the following question: how much does the number field generated by the sum $x + y$ or the product xy of two singular moduli differ from the field $\mathbb{Q}(x, y)$? The objective of this note is to show that the fields $\mathbb{Q}(x + y)$ and $\mathbb{Q}(xy)$ (provided $xy \ne 0$) are subfields of $\mathbb{Q}(x, y)$ of degree at most 2, and in "most cases" each of $x + y$ and xy generates $\mathbb{Q}(x, y)$. Here are our principal results.

Theorem 1.2. *Let x and y be singular moduli. Then $\mathbb{Q}(x + y) = \mathbb{Q}(x, y)$ if $\Delta_x \ne \Delta_y$, and $[\mathbb{Q}(x, y) : \mathbb{Q}(x + y)] \le 2$ if $\Delta_x = \Delta_y$.*

Theorem 1.3. *Let x and y be non-zero singular moduli. Then $\mathbb{Q}(xy) = \mathbb{Q}(x, y)$ if $\Delta_x \ne \Delta_y$, and $[\mathbb{Q}(x, y) : \mathbb{Q}(xy)] \le 2$ if $\Delta_x = \Delta_y$.*

Both the "sum" and the "product" statements of Theorem 1.1 are very special cases of these two theorems.

Note that in the case $\Delta_x = \Delta_y$, the statements $[\mathbb{Q}(x, y) : \mathbb{Q}(x + y)] \le 2$ and $[\mathbb{Q}(x, y) : \mathbb{Q}(xy)] \le 2$ are best possible: one cannot expect that $x + y$ or xy always generates $\mathbb{Q}(x, y)$

Please cite this article in press as: B. Faye, A. Riffaut, Fields generated by sums and products of singular moduli, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.03.015