FIELDS GENERATED BY SUMS AND PRODUCTS OF SINGULAR MODULI: THE PRIMITIVE ELEMENT PROBLEM

BERNADETTE FAYE

Abstract. 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, $[\mathbb{Q}(x) : \mathbb{Q}] = h(\Delta_x)$.

Here, 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. Futhermore, we fix a rational number $\alpha \neq 0, \pm 1$ and show that the field $\mathbb{Q}(x, y)$ is generated by $x + \alpha y$, with a few exceptions occurring when x and y generate the same quadratic field over $\mathbb{Q}$.

These are the results from my collaborations with Antonin Riffault, Yuri Bilu and Huilin Zhu.

keywords: André Oort Conjecture, Curves with complex multiplication, j.invariant.