Vol. 54, No. 1 DUKE MATHEMATICAL JOURNAL © 1987

REPRESENTATION THEORY AND THE CUSPIDAL GROUP OF $X(p)$

BENEDICT H. GROSS

To Yu. I. Manin

Let p be a prime number, and let $X(p)$ denote the modular curve which classifies elliptic curves with a level p structure. Then $X(p)$ is a normal covering of the moduli $X(1)$ of elliptic curves, with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm 1 \rangle$. Hecke used the complex representation theory of the geometric Galois group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm 1 \rangle$ to study certain holomorphic differentials on $X(p)$ [1; §7, 8]. In this note we will use the representation theory of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ in characteristic p to study the cuspidal subgroup C in the Jacobian.

A general argument due to Manin and Drinfeld shows that C is a finite group [3, Cor. 3.6], and Kubert and Lang have obtained a formula for its order [2, pg. 118]. Here we will determine the structure of $C \otimes \mathbb{Z}_p$ as a module over the Galois group of $X(p)$. In particular, using the non semi-simplicity of certain modular representations of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, we will show that for $p \geqslant 5$ the quotient C/pC has dimension $\geqslant (p-5)(p-1)/4$ over $\mathbb{Z}/p\mathbb{Z}$, with equality holding if and only if the prime p is regular.

§1. The canonical model of $X(p)$. In this section, we recall some basic facts about the curve $X(p)$. The proofs may be found in the books of Kubert-Lang [2] and Shimura [5, Ch. 6].

The moduli $X(1)$ of elliptic curves is defined over $\mathbb{Q}$ and has function field $k = \mathbb{Q}(j)$, where j is Dedekind's modular function. Let E be an elliptic curve over k with invariant $j(E) = j$. Let L be the normal extension of k which is generated by the co-ordinates of the nontrivial p-division points on E over $\bar{k}$. The Galois group of L over k acts $\mathbb{Z}/p\mathbb{Z}$-linearly on E_p, and this representation gives an isomorphism: $\mathrm{Gal}(L/k) \simeq \mathrm{Aut}(E_p)$. If we fix an isomorphism $E_p \simeq (\mathbb{Z}/p\mathbb{Z})^2$ by choosing a basis of E_p over $\mathbb{Z}/p\mathbb{Z}$, we obtain an isomorphism $\mathrm{Gal}(L/k) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

The group $\mathrm{Aut}(E) = \langle \pm 1 \rangle$ embeds as a subgroup of $\mathrm{Aut}(E_p)$, so acts on the field L. We let K be the fixed field; then K is generated over k be the x-co-ordinates of the nontrivial p-division points: $x_a = x_{-a}$ for $a \in A = E_p - \{0\}/\langle \pm 1 \rangle$. The field K is normal over k and, unlike L, is independent of the curve E chosen with invariant j. We have a canonical isomorphism $G =$

Received November 29, 1986.