On the component groups and the Shimura subgroup of J ...
(N)
by RIBET, K.
in Seminaire de Théorie des Nombres de Bordeaux
volume 16; pp. 1 - 10

Göttingen State and University Library

Terms and Conditions

The Göttingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Göttingen State- and University Library.
Each copy of any part of this document must contain these Terms and Conditions.With the usage of the library's online-systems to access or download a digitizied document you accept these Terms and Conditions.

Reproductions of materials on the web site may not be made for or donated to other repositories, nor may they be further reproduced without written permission from the Göttingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:
Niedersaechsische Staats- und Universitaetsbibliothek Göttingen
Digitalisierungszentrum
37070 Göttingen
Germany
E-Mail: gdz@www.sub.uni-goettingen.de

Purchase a CD-ROM

The Goettingen State and University Library offers CD-ROMs containing whole volumes / monographs in PDF for Adobe Acrobat. The PDF-version contains the table of contents as bookmarks, which allows easy navigation in the document. For availability and pricing, please contact:

Niedersaechsische Staats- und Universitaetsbibliothek Göttingen
Digitalisierungszentrum
37070 Göttingen
Germany
E-Mail: gdz@www.sub.uni-goettingen.de

Göttingen State and University Library

Göttinger Digitalisierungs-Zentrum

Séminaire de Théorie des Nombres de Bordeaux
Année 1987-1988 - Exposé n° 6 le 30 octobre 1987

ON THE COMPONENT GROUPS AND THE SHIMURA SUBGROUP OF $J_0(N)$

by

Kenneth A. RIBET

Let N be a positive integer, and let p be a prime number which is prime to N. Consider the usual modular curves $X_o(N)$ and $X_o(pN)$ over $\mathbf{Q}$. Recall that there are two natural degeneracy maps

$$X_o(pN) \rightrightarrows X_o(N),$$

cf. [7]. If we regard the modular curves as classifying elliptic curves with $\Gamma_o(pN)$- and $\Gamma_o(N)$-structures, respectively, then we may interpret these maps as follows:

> An elliptic curve with a $\Gamma_o(pN)$-structure may be thought of as a triple (E, C_N, C_p), where E is an elliptic curve, and C_N and C_p are cyclic subgroups on E, of order N and p, respectively. Forgetting the subgroup C_p, we obtain the pair (E, C_N), which is an elliptic curve with a $\Gamma_o(N)$-structure. This construction defines one of the two degeneracy maps. To define the other, we divide E by its subgroup C_p, thereby obtaining a second elliptic curve E'. The image of C_N on E' is a cyclic subgroup C'_N on E', and the pair (E', C'_N) is the image of (E, C_N, C_p) under the second degeneracy map.

We recall also that either of these degeneracy maps may be obtained from the other by composition with the Atkin-Lehner involution w_p of $X_o(Np)$. This involution attaches to (E, C_N, C_p) the triple consisting of E', C'_N, and the image C'_p on E' of the kernel of multiplication by p on E.

Let J and J' be the Jacobians

$$J = \mathrm{Pic}^o(X_o(N)), \qquad J' = \mathrm{Pic}^o(X_o(pN)).$$

The two degeneracy maps introduced above induce by Pic functoriality a pair of degeneracy maps

$$\alpha, \beta : J \rightrightarrows J',$$

where α corresponds to the first construction discussed above, and β to the second. By Albanese functoriality, they induce a second pair of maps

$$\check{\alpha}, \check{\beta} : J' \rightrightarrows J.$$

These may be considered as the homomorphisms of abelian varieties dual to α and β, respectively, once the abelian varieties J and J' are identified with their own duals (autoduality of the Jacobian).

The four maps satisfy $\check{\alpha} \circ \alpha = \check{\beta} \circ \beta = p + 1$, since the initial degeneracy maps are coverings of curves of degree $p + 1$. At the same time, we have the formulas

$$\check{\alpha} \circ \beta = \check{\beta} \circ \alpha = T_p$$

on J, where T_p is the indicated Hecke operator. These latter formulas follow directly from the geometric definition of T_p.

In particular, suppose that Δ is a subgroup of J on which the relation $\alpha = \beta$ holds. Applying $\check{\beta}$ or $\check{\alpha}$, we deduce that the formula $T_p = p + 1$ holds on Δ. Especially, if the relation $\alpha = \beta$ is satisfied for each p prime to N, the group Δ is *Eisenstein* in the sense of Mazur's article [5]: we have $T_p = 1 + p$ for all p prime to N.

The purpose of this note is to illustrate this theme in two contexts. First, recall the natural covering of modular curves

$$\pi : X_1(N) \to X_o(N). \tag{1}$$

By Pic functoriality, this covering induces a map

$$\pi^* : J \to J_1(N).$$

The kernel Σ_N of this homomorphism is the *Shimura subgroup* of $J_o(N)$.

Theorem 1. *The relation $\alpha = \beta$ holds on Σ_N. In particular, Σ_N is Eisenstein.*

Theorem 1 is nothing but the "easy half" of the Theorem 4.3 of the author's article [11]. As explained in [11], the Theorem follows easily from the assertion that the Atkin-Lehner operator w_N of $J_o(N)$ operates on Σ_N by the scalar -1. This latter assertion is proved by Mazur in [5] (Proposition 11.7, page 100) in a context where N is supposed prime. In [11], I remarked that Mazur's argument in fact works for arbitrary N. We will verify this below (Lemma 1).

In the second result of this note, we suppose that N is a product Mq, where q is a prime number which is prime to M. Consider the fibers over $\mathbf{F}_q$ of the Néron models of J and J'. These "special fibers" are extremely well understood, thanks to the work of Deligne-Rapoport [1] and Raynaud [10]. They are commutative group schemes which are not (necessarily) connected. Let Φ and Φ' be the groups of components of the special fibers of J and J', respectively. As we recall below, the groups Φ and Φ' are finite abelian groups which can be expressed in terms of the supersingular points of $X_o(M)$ and $X_o(pM)$ in characteristic q [8].

The maps α and β induce by functoriality homomorphisms $\alpha_*, \beta_*: \Phi \rightrightarrows \Phi'$.

Theorem 2. *The maps α_* and β_* are equal. In particular, the group Φ is Eisenstein.*

Theorem 2 has recently been generalized by B. Edixhoven [2] to the case where q is not necessarily prime to M. Edixhoven bases his work on the results of Katz-Mazur [4] and his subsequent study of the regular minimal models of modular curves.

1 Proof of Theorem 1

The proof employs various familiar operators on the two modular curves $X_o(N)$ and $X_1(N)$, cf. for example [9], Chapter 2, §5 and [6], §1. The *diamond bracket* operators are the elements of the Galois group Δ of the covering (1). This group is the quotient of $(\mathbf{Z}/N\mathbf{Z})^*$ by its subgroup con-

sisting of ± 1, and we write $\langle a \rangle$ for the image in Δ of an integer a prime to N.

Next we have the *Atkin-Lehner* involutions w_Q on $X_o(N)$ for each positive divisor Q of N satisfying $(Q, N/Q) = 1$. The operator w_Q of $X_o(N)$ corresponds to the construction which maps an elliptic curve E with a cyclic subgroup C of order N to the pair $\big(E/C[Q], (C[N/Q] \oplus E[Q])/C[Q]\big)$. (Here, the bracket notation $G[n]$ is used to denote the kernel of multiplication by n on an abelian group G.) We write simply w for w_N.

Finally, we recall that an involution $w = w_N$ can be defined on $X_1(N)$, once a primitive N^{th} root of unity $\zeta \in \overline{\mathbf{Q}}^*$ is fixed. Here, one regards $X_1(N)$ as classifying pairs (E, P), where P is a point of order N on E. Given such a pair, choose $Q \in E[N]$ such that $\langle P, Q \rangle_N = \zeta$, where $\langle\ ,\ \rangle_N$ is the Weil pairing. Let $\bar{E}$ be the quotient of E by the subgroup of E generated by P, and let $\bar{Q}$ be the image of Q on $\bar{E}$. The involution w maps (E, P) to $(\bar{E}, \bar{Q})$.

The operator w on $X_1(N)$ and the diamond-bracket operators are linked by the easily established commutation relation

$$w \langle a \rangle w = \langle a \rangle^{-1}.$$

We consider that these operators act on the Jacobians $J = J_o(N)$ and $J_1(N)$ of $X_o(N)$ and $X_1(N)$ by Pic functoriality.

Lemma 1. *The involution w acts on the Shimura subgroup Σ of J by multiplication by -1.*

Proof. Let D be a divisor of degree 0 on $X_o(N)$ whose class in $J_o(N)$ lies in Σ. By the definition of the Shimura subgroup of J, there is a function f on $X_1(N)$ such that $\pi^{-1}(D) = (f)$. The invariance of (f) under the $\langle a \rangle$ shows that we have $f \circ \langle a \rangle = \epsilon(a) f$ for all $a \in (\mathbf{Z}/N\mathbf{Z})^*$, where ϵ is some character $(\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{Q}}^*$.

The product of f with the composition $f \circ w$ is then invariant under the $\langle a \rangle$ and is thus a function on $X_o(N)$. Its divisor is $D + wD$. ∎

We now may prove Theorem 1 by applying the Lemma to J and J'. Indeed, we have clearly $\alpha(\Sigma_N) \subseteq \Sigma_{Np}$, so that the Lemma implies that w_{Np} acts on $\alpha(\Sigma_N)$ by -1. Because α "commutes" with the Atkin-Lehner operators w_N on $X_o(N)$ and on $X_o(Np)$, the Lemma also shows that w_N

acts on $\alpha(\Sigma_N)$ by -1. Hence w_p acts on $\alpha(\Sigma_N)$ by +1. Since $\beta = w_p \circ \alpha$, Theorem 1 follows.

2 Automorphisms of Elliptic Curves

In this §, we suppose that q is a prime number. Let k be an algebraically closed field of characteristic q, and let E be a supersingular elliptic curve over k. According to a well known theorem of M. Deuring, the endomorphism algebra

$$\mathcal{H} = \mathrm{End}(E) \otimes \mathbf{Q}$$

of E is a (definite) quaternion algebra over $\mathbf{Q}$ of discriminant q. The ring $\mathrm{End}(E)$ is known to be a maximal order in $\mathcal{H}$. Consider the group $\mathrm{Aut}(E)$ of units of $\mathrm{End}(E)$. This group contains the subgroup $\{\pm 1\}$, and it is clear that any element ϵ of $\mathrm{Aut}(E)$ which is different from ± 1 must have order 4 or 6. Indeed, the subalgebra K of $\mathcal{H}$ generated by ϵ must be an *imaginary* quadratic field, since $\mathcal{H}$ is a definite quaternion algebra. The subring $\mathbf{Z}[\epsilon]$ of $\mathrm{End}(E)$ is then an order in K, so that its unit group is one of the three groups $\mu_2 = \{\pm 1\}$, μ_4, μ_6.

Let C be a finite subgroup of $E(k)$. Let $\mathrm{End}(E, C)$ denote the ring of endomorphisms of E which preserve C. Then $\mathrm{End}(E, C)$ has finite index in $\mathrm{End}(E)$, so it is again an order in $\mathcal{H}$. Its group of units $\mathrm{Aut}(E, C)$ is a subgroup of $\mathrm{Aut}(E)$ which contains the group $\{\pm 1\}$.

Proposition 1. *Suppose that* $\mathrm{Aut}(E, C)$ *contains an element* $\epsilon \neq \pm 1$. *Then the elliptic curves* E *and* E/C *are isomorphic.*

Proof. Let R be the subring $\mathbf{Z}[\epsilon]$ of $\mathrm{End}(E, C)$. As noted above, ϵ has order 3, 4, or 6, and $K = R \otimes \mathbf{Q}$ is either the field of fourth or of sixth roots of unity. Hence R is the ring of integers of K, and therefore a principal ideal domain. Let n be the exponent of C, so that C is in particular a subgroup of the kernel $E[n]$ of multiplication by n on E. It is clear that the action of R on E makes $E[n]$ a free rank-1 module over R/nR. This follows, for instance, from the standard fact that the Tate module $T_\ell(E)$ is free of rank 1 over $R \otimes \mathbf{Z}_\ell$ for each prime $\ell \neq q$.

Fixing an R-isomorphism between $E[n]$ and R/nR, we may identify C with the quotient I/nR, for some ideal I of R containing n. Since R is

a principal ring, there is an element $r \in R$ such that $nR = rI$. Then C coincides with the kernel $E[r]$ of multiplication by r on E. Indeed, this kernel is contained in $E[n]$, since n is divisible by r. Computing in the group of fractional ideals of R, we see that I/nR is the kernel of multiplication by r on R/nR. It follows that C is the kernel of multiplication by r on $E[n]$.

The statement of the Proposition now follows, since multiplication by r induces an isomorphism between E/C and E. ∎

As a variant, we suppose given a second finite group D of $E(k)$ whose intersection with C is trivial. Write $\overline{E}$ for E/C, and let $\overline{D}$ be the image $(D \oplus C)/C$ of D on $\overline{E}$.

Proposition 2. *Suppose that there is an automorphism $\epsilon \neq \pm 1$ of E which preserves each of C and D. Then there is an isomorphism $E \approx \overline{E}$ which takes D to $\overline{D}$.*

Proof. Let R and r be as in the proof of Proposition 1. The endomorphism r of E then maps D to itself. When we view r as a map $E/C \to E$, r maps the subgroup $\overline{D}$ of E/C to the subgroup D of E. This sets up an isomorphism as claimed, since $\overline{D}$ and D have the same order. ∎

3 Monodromy Pairings

In this §, we recall the combinatorial desciptions of Φ and Φ' which were alluded to above. We assume that M, q,... are as in the statement of Theorem 2. We take k to be an algebraic closure of $\mathbf{F}_q$.

Let $\mathcal{S}$ be the set of k-valued supersingular points of $X_o(M)$. Thus $\mathcal{S}$ is the set of isomorphism classes of pairs (E, C_M), where E is a supersingular elliptic curve over k and $C_M \subset E$ is a cyclic subgroup of order M. For each such pair, pose

$$\kappa(E, C_M) = \frac{1}{2}\#\mathrm{Aut}(E, C_M).$$

The formula

$$\langle \sum_{s \in \mathcal{S}} n_s s, \sum_{s \in \mathcal{S}} m_s s \rangle = \sum_{s \in \mathcal{S}} n_s m_s \kappa(s)$$

defines a bilinear pairing on $\mathbf{Z}^{\mathcal{S}}$. Let $X \subset \mathbf{Z}^{\mathcal{S}}$ be the group of degree-0 divisors on $\mathcal{S}$. Let $\langle\ ,\ \rangle_X$ be the restriction of the pairing $\langle\ ,\ \rangle$ to X. We

view $\langle\ ,\ \rangle_X$ as an injection

$$\iota_X : X \hookrightarrow X^*,$$

where $X^* = \mathrm{Hom}(X, \mathbf{Z})$.

Formula. *The component group Φ is the cokernel of ι_X.*

A general formula of this type was deduced by Grothendieck in SGA7 from the work of Raynaud [10]. (See [3], 12.5 and 12.10.) To apply it to $J_o(qM)_{\mathbf{F}_q}$, one uses the description given by Deligne-Rapoport [1] of $X_o(qM)$ over $\mathbf{Z}_q$.

By analogy, we have a similar description of Φ' in which $\mathcal{S}$ is replaced by $\mathcal{S}'$, the set of isomorphism classes of triples (E, C_M, C_p), where C_p is a cyclic subgroup of E of order p. We let L and $\langle\ ,\ \rangle_L$ be the analogues of X and $\langle\ ,\ \rangle_X$. The pairing $\langle\ ,\ \rangle_L$ on $L \times L$ may be viewed as an injection

$$\iota_L : L \hookrightarrow L^*,$$

whose cokernel is Φ'.

In the descriptions of Φ and Φ', the groups X and L intervene as character groups of tori. In general, if A is an abelian variety over $\mathbf{Q}_q$ which has semistable reduction, we let $X(A)$ be the free finite-rank abelian group which is defined as follows. The special fiber of the Néron model of A is an extension of a finite "group of components" $\Phi(A)$ by a connected semi-abelian variety A°. This latter object is in turn an extension of an abelian variety by a torus T, and we let

$$X(A) = \mathrm{Hom}_k(T, \mathsf{G_m})$$

be its character group. From the results of [1] and §12.3 of [3], we find canonical isomorphisms

$$X(J) \approx X, \qquad X(J') \approx L.$$

For each A with semistable reduction, there is a monodromy pairing

$$\langle\ ,\ \rangle_A : X(A) \times X(A^t) \to \mathbf{Z},$$

where A^t is the abelian variety dual to A. This pairing may be regarded as an injection

$$\iota_A : X(A^t) \to X(A)^*,$$

and the cokernel of this injection is the group $\Phi(A)$. Given a homomorphism $f\colon A \to B$ between abelian varieties with semistable reduction, we may read off $f_* : \Phi_A \to \Phi_B$ from a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & X(A^t) & \to & X(A)^* & \to & \Phi(A) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & X(B^t) & \to & X(B)^* & \to & \Phi(B) & \to & 0. \end{array}$$

Here the map $X(A^t) \to X(B^t)$ corresponds to the map on tori induced by the homomorphism $f^t\colon A^t \to B^t$ dual to f, while the map $X(A)^* \to X(B)^*$ is $\mathrm{Hom}(f^*, \mathbf{Z})$, where $f^*\colon X(B) \to X(A)$ corresponds to the map on tori induced by f.

This general description specializes to a concrete interpretation of the maps $\alpha_*, \beta_*\colon \Phi \rightrightarrows \Phi'$. The Jacobians J and J' are each naturally autodual, so that α^t and β^t are each homomorphisms $J' \to J$. These homomorphisms are in fact $\check{\alpha}$ and $\check{\beta}$, because of the general principle that maps on Jacobians induced by Pic functoriality are dual to maps on Jacobians induced by Albanese functoriality. The maps on character groups

$$\alpha^*, \beta^* : L \rightrightarrows X, \qquad \check{\alpha}^*, \check{\beta}^* : X \rightrightarrows L$$

may be computed using the ideas of [10].

The result of the computation, which is easy to guess, is as follows. Let $\sigma\colon \mathcal{S}' \to \mathcal{S}$ and $\tau\colon \mathcal{S}' \to \mathcal{S}$ be the (degeneracy) maps which take (E, C_M, C_p) to (E, C_M) and $\big(E/C_p, (C_M \oplus C_p)/C_p\big)$, respectively. These define a pair of linear maps $\mathbf{Z}^{\mathcal{S}'} \rightrightarrows \mathbf{Z}^{\mathcal{S}}$ and then, by restriction, two maps $L \rightrightarrows X$. These homomorphisms are α^* and β^*, with α corresponding to σ and β to τ. On the other hand, the map $\check{\alpha}^*\colon X \to L$ is induced from the linear map $\mathbf{Z}^{\mathcal{S}} \to \mathbf{Z}^{\mathcal{S}'}$ which maps (E, C_M) to the formal sum

$$\sum_{C_p} (E, C_M, C_p)$$

in which C_p runs over the $p+1$ different subgroups of E of order p. A similar description is available for $\check{\beta}^*$.

For later use, we introduce the notation w for the Atkin-Lehner involution $w_p\colon \mathcal{S}' \to \mathcal{S}'$. It is given explicitly by the formula

$$(E, C_M, C_p) \mapsto \big(E/C_p, (C_M \oplus C_p)/C_p, E[p]/C_p\big).$$

This involution satisfies $\alpha^* \circ w = \beta^*$ and $w \circ \check{\alpha}^* = \check{\beta}^*$.

4 Proof of Theorem 2

Consider the map $\eta = \mathrm{Hom}(\alpha^* - \beta^*, \mathbf{Z}) : X^* \to L^*$. Using the description provided above, we readily see that the Theorem 2 amounts to the following statement: *The image of η is contained in the image of ι_L: $L \to L^*$.* To prove this fact, we consider an arbitrary element φ of X^*. For convenience, we lift φ to a linear form on $\mathbf{Z}^{\mathcal{S}}$, which we again call φ. Let ℓ be the sum

$$\sum_{s \in \mathcal{S}'} \varphi(\sigma s - \tau s) \cdot s \in \mathbf{Z}^{\mathcal{S}'}.$$

The degree of ℓ is the difference

$$\sum_{s \in \mathcal{S}'} \varphi(\sigma s) - \sum_{s \in \mathcal{S}} \varphi(\tau s).$$

The two sums are, however, equal, since we have $\sigma \circ w = \tau$ and since w is a permutation of $\mathcal{S}'$. Hence ℓ has degree 0, which is to say that it is an element of L. We shall establish the equality

$$\iota_L(\ell) = \eta(\varphi),$$

thereby verifying that $\eta(\varphi)$ is in the image of ι_L.

To prove this formula, take two elements y_1 and y_2 of $\mathcal{S}'$. We must show

$$\langle \ell, y_1 - y_2 \rangle_L \stackrel{?}{=} \eta(\varphi)(y_1 - y_2).$$

The left-hand side of this desired equality is the difference

$$\varphi(\sigma y_1 - \tau y_1) \cdot \kappa(y_1) \; - \; \varphi(\sigma y_2 - \tau y_2) \cdot \kappa(y_2).$$

The right-hand side of the equality is identical to this difference, except that the factors $\kappa(y_i)$ do not appear. Hence it suffices to record the following

Lemma. *Let $y \in \mathcal{S}'$. Suppose that we have $\kappa(y) > 1$. Then $\sigma y = \tau y$.*

This Lemma in fact follows immediately from Proposition 2 when we choose $C = C_p$ and $D = C_M$ in the notation of that Proposition.

References

[1] Deligne, P. and Rapoport, M. Les schémas de modules de courbes elliptiques. *Lecture Notes in Math* **349**, 143–316 (1973)

[2] Edixhoven, B. To appear.

[3] Grothendieck, A. SGA7 I, Exposé IX. *Lecture Notes in Math.* **288**, 313–523 (1972)

[4] Katz, N.M. and Mazur, B. Arithmetic Moduli of Elliptic Curves. *Annals of Math. Studies* **108**. Princeton: Princeton University Press, 1985

[5] Mazur, B. Modular curves and the Eisenstein ideal. *Publ. Math. IHES* **47**, 33–186 (1977)

[6] Kenku, M.A. and Momose, F. Automorphism groups of the modular curves $X_0(N)$. *Compositio Math.* **65**, 51–80 (1988)

[7] Mazur, B. Rational isogenies of prime degree. *Invent. Math.* **44**, 129–162 (1978)

[8] Mazur, B. and Rapoport, M. Behavior of the Néron model of the jacobian of $X_o(N)$ at bad primes. Appendix to [5].

[9] Mazur, B. and Wiles, A. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.* **76**, 179–330 (1984)

[10] Raynaud, M. Spécialisation du foncteur de Picard. *Publ. Math. IHES* **38**, 27–76 (1970)

[11] Ribet, K. Congruence relations between modular forms. Proc. International Congress of Mathematicians 1983, 503–514

(Texte reçu le 7 juin 1988)

K. RIBET

University of California
BERKELEY
CALIFORNIA 94720
U.S.A.