The Shimura Subgroup of $J_0(N)$

San Ling* and Joseph Oesterlé†

SUMMARY. — *To the natural morphism $X_1(N) \to X_0(N)$ of modular curves corresponds, by Picard functoriality, a morphism $J_0(N) \to J_1(N)$ between their Jacobian varieties. Its kernel $\Sigma(N)$, called the Shimura subgroup of $J_0(N)$, is finite. We determine the group structure of $\Sigma(N)$ together with the action of Galois and the action of the Hecke algebra. This extends previous results obtained by B. Mazur and K. Ribet.*

Let $N \geq 1$ be an integer and let $\Gamma_0(N)$ be the subgroup of $SL_2(\mathbf{Z})$ consisting of the matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ such that N divides c. It acts on the Poincaré half-plane $\mathcal{H} = \{\tau \in \mathbf{C} |\ \operatorname{Im}\tau > 0\}$ and on $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ by

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ \tau \right) \mapsto \frac{a\tau + b}{c\tau + d}.$$

The quotient $X_0(N) = \Gamma_0(N)\backslash\overline{\mathcal{H}}$ has a natural structure of compact connected Riemann surface.

One defines in a similar way a Riemann surface $X_1(N) = \Gamma_1(N)\backslash\overline{\mathcal{H}}$, where $\Gamma_1(N)$ is the subgroup of $\Gamma_0(N)$ consisting of the matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a \equiv d \equiv 1 \bmod N$. Let $u : X_1(N) \to X_0(N)$ be the holomorphic map deduced from the identity on $\overline{\mathcal{H}}$ by passing to the quotients.

*This research was financially supported by the National University of Singapore Overseas Graduate Scholarship. The author wishes to thank Ken Ribet for helpful discussion.

†This work was completed while the author was a visiting professor at the Miller Institute for Basic Research in Science in Berkeley.

S.M.F.
Astérisque 196-197 (1991)

Let $J_0(N)$ and $J_1(N)$ be the Jacobian varieties of $X_0(N)$ and $X_1(N)$, viewed as the connected components of 0 in the corresponding Picard varieties. Let

$$u^* : J_0(N) \longrightarrow J_1(N)$$

be the morphism of abelian varieties deduced from u by Picard functoriality. Its kernel, called the *Shimura subgroup* of $J_0(N)$, is a finite group; we denote it by $\Sigma(N)$.

In this paper, we give a complete description of $\Sigma(N)$: group structure, exponent, order, action of Galois, of Atkin-Lehner involutions and of Hecke operators (including those associated to the primes dividing N), behaviour under degeneracy maps, etc. This extends previous results obtained by B. Mazur ([3], II, 11) and K. Ribet ([5]). Our proofs are of complex analytic nature and would apply in situations where $\Gamma_0(N)$ and $\Gamma_1(N)$ are replaced by discrete subgroups of $SL_2(\mathbf{R})$ of finite covolume, even when the corresponding Riemann surfaces have no modular interpretation.

Let $\mathbf{U}$ be the group of complex numbers of modulus 1. We define in §1 a canonical injective group homomorphism

$$\psi : J_0(N) \longrightarrow \mathrm{Hom}(\Gamma_0(N), \mathbf{U}). \tag{1}$$

Throughout the paper, we identify the group $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma_1(N) \mapsto d + N\mathbf{Z}.$$

We show that an element x of $J_0(N)$ belongs to the Shimura subgroup $\Sigma(N)$ if and only if the kernel of $\psi(x)$ contains $\Gamma_1(N)$. Therefore, we deduce from ψ a canonical injective homomorphism

$$\psi' : \Sigma(N) \longrightarrow \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}). \tag{2}$$

We determine its image in §2 and obtain:

THEOREM 1 .— *The Shimura subgroup $\Sigma(N)$ of $J_0(N)$ is canonically isomorphic to the group of homomorphisms $g : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{U}$ such that $g(d) = 1$ if $d = -1$, $d^2 + 1 = 0$, $d^2 + d + 1 = 0$ or $(d-1)^2 = 0$.*

By using thm. 1, we compute in §3 the order and the exponent of the group $\Sigma(N)$:

COROLLARY 1 .— *Let $\phi(N)$ denote the number of elements of $(\mathbf{Z}/N\mathbf{Z})^\times$ and:*

(i) let m be the largest integer such that m^2 divides N;

(ii) let k be the number of prime divisors of N distinct from 2 and 3;

(iii) let m_2 be equal to 2 if -1 is a square mod N *(i.e., if $4 \nmid N$ and each prime factor $p \neq 2$ of N is congruent to* 1 mod 4*), and let m_2 be equal to* 1 *otherwise;*

(iv) let m_3 be equal to 3 if $X^2 + X + 1$ has a root mod N *(i.e., if $9 \nmid N$ and each prime factor $p \neq 3$ of N is congruent to* 1 mod 3*), and let m_3 be equal to* 1 *otherwise.*

Then we have

$$\mathrm{Card}(\Sigma(N)) = \begin{cases} \phi(N)/(2mm_2^k m_3^k) & \text{if } N \geq 5 \\ 1 & \text{if } N \leq 4. \end{cases}$$

EXAMPLE.— If N is of the form p^n, with p a prime number and $n \geq 1$, then $\Sigma(N)$ is a cyclic group (thm. 1). If $p \neq 2$, its order is the product of $p^{n-1-[n/2]}$ and the numerator of $\frac{p-1}{12}$; if $p = 2$, its order is $2^{\max(0,n-2-[n/2])}$.

COROLLARY 2 .— *Let $N = \prod p^{r_p}$ be the prime power decomposition of N and:*

(i) let r'_p be equal to $r_p - 1 - [r_p/2]$ if $p \neq 2$;

(ii) let r'_2 be equal to $\max(0, r_2 - 2 - [r_2/2])$;

(iii) let e_0 be equal to $\operatorname{lcm}_{p|N}((p-1)p^{r'_p})$;

(iv) let m_1 be equal to 2 if N is the product of 1, 2 or 4 by a power of an odd prime, and let m_1 be equal to 1 otherwise;

(v) let m_2 and m_3 be as in cor. 1.

Then the exponent of the group $\Sigma(N)$ (i.e., the smallest integer e such that $e\Sigma(N) = 0$) is given by

$$e = \begin{cases} e_0/(m_1 m_2 m_3) & \text{if } N \geq 5 \\ 1 & \text{if } N \leq 4. \end{cases}$$

COROLLARY 3 .— *The only integers N for which the order of $\Sigma(N)$ is* 1 *are* 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25, 36, 49, 50 *and* 169.

In fact, for all these values of N except 36, 49, 50 and 169, the genus of the Riemann surface $X_0(N)$ is 0 and we therefore have $J_0(N) = 0$.

COROLLARY 4 .— *When N approaches infinity, the exponent and a fortiori the order of $\Sigma(N)$ go to infinity.*

The Riemann surface $X_0(N)$ is the group of complex points of a modular curve $X_0(N)_{\mathbf{Q}}$ defined over $\mathbf{Q}$. Therefore, $J_0(N)$ is naturally defined over $\mathbf{Q}$ and the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, where $\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, acts on the group of torsion points of $J_0(N)$. It acts, in particular, on the Shimura subgroup $\Sigma(N)$. We determine this action in §4, and obtain:

THEOREM 2 .— *Let e be the exponent of the group $\Sigma(N)$ (see* cor. 2 *of* thm. 1*). The smallest common field of definition of the points of $\Sigma(N)$ is the cyclotomic field $\mathbf{Q}(\mu_e)$. The Galois group $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q})$ acts on $\Sigma(N)$ via the cyclotomic character $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q}) \to (\mathbf{Z}/e\mathbf{Z})^\times$.*

COROLLARY 1 .— *A point x of $\Sigma(N)$ is rational over $\mathbf{Q}$ if and only if we have $2x = 0$. The number of those points is $2^{\mathrm{Card}(P)+\epsilon}$, where P is the set of odd primes dividing N and ϵ is given by*

$$\epsilon = \begin{cases} -1 & \text{if } 4 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 8; \\ -1 & \text{if } 4|N,\ 8 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 4; \\ 1 & \text{if } 32|N; \\ 0 & \text{otherwise.} \end{cases}$$

COROLLARY 2 .— *The only integers N for which all points of $\Sigma(N)$ are rational over $\mathbf{Q}$ are:*

(i) those for which $\Sigma(N)$ is of order 1, *listed in* cor. 3 *of* thm. 1*;*

(ii) the integers $20, 21, 24, 32, 48, 64, 72, 100, 144$ *and* 147, *for which $\Sigma(N)$ is of order* 2*;*

(iii) the integers $96, 192, 288$ *and* 576, *for which $\Sigma(N)$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$.*

To each divisor N_1 of N, such that N_1 is prime to N/N_1, is associated an *Atkin-Lehner involution* w_{N_1} of $X_0(N)$: for the definition, see §5. The involutions ${w_{N_1}}^*$ and $(w_{N_1})_*$ of $J_0(N)$ deduced by Picard and Albanese functorialities respectively coincide. The behaviour of the Shimura subgroup of $J_0(N)$ under these maps is studied in §5. We obtain:

THEOREM 3 .— *The Shimura subgroup $\Sigma(N)$ of $J_0(N)$ is stable under ${w_{N_1}}^*$. Moreover, we have the commutative diagram*

$$\begin{array}{ccc} \Sigma(N) & \xrightarrow{\psi'} & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}) \\ \alpha \downarrow & & {}^t\alpha' \downarrow \\ \Sigma(N) & \xrightarrow{\psi'} & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}), \end{array} \tag{3}$$

where α is the map induced by ${w_{N_1}}^*$, ψ' is the canonical injection (2), and ${}^t\alpha'$ is the transpose of the involution $\alpha' : (\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/N\mathbf{Z})^\times$ which coincides with $t \mapsto t^{-1}$ modulo N_1 and with the identity modulo N/N_1.

The following particular case of thm. 3 was previously obtained by K. Ribet ([5], lemma 1):

COROLLARY .— *The involution ${w_N}^*$ acts on the Shimura subgroup $\Sigma(N)$ by multiplication by -1.*

Let M be a divisor of N. For each divisor D of N/M, we have a holomorphic degeneracy map $v_D : X_0(N) \to X_0(M)$. It is the map deduced from the transformation $\tau \mapsto D\tau$ of $\overline{\mathcal{H}}$ by passing to the quotients; a modular definition of v_D is given in §6. By Picard and Albanese functorialities respectively, we get morphisms of abelian varieties

$$\begin{aligned} {v_D}^* &: J_0(M) \longrightarrow J_0(N), \\ (v_D)_* &: J_0(N) \longrightarrow J_0(M), \end{aligned} \tag{4}$$

the latter being the dual of the former. The behaviour of the Shimura subgroups under these maps is studied in §6. We obtain:

THEOREM 4 .— *We have ${v_D}^*(\Sigma(M)) \subseteq \Sigma(N)$. Moreover, we have the commutative diagram*

$$\begin{array}{ccc} \Sigma(M) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/M\mathbf{Z})^\times, \mathbf{U}) \\ \beta \downarrow & & {}^t\beta' \downarrow \\ \Sigma(N) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}), \end{array} \tag{5}$$

where β is the map induced by ${v_D}^*$, the horizontal arrows represent the canonical injections (2), and ${}^t\beta'$ is the transpose of the canonical surjection $\beta' : (\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/M\mathbf{Z})^\times$.

THEOREM 5 .— *We have $(v_D)_*(\Sigma(N)) \subseteq \Sigma(M)$. Moreover, we have the commutative diagram*

$$\begin{array}{ccc} \Sigma(N) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}) \\ \delta \downarrow & & {}^t\delta' \downarrow \\ \Sigma(M) & \longrightarrow & \mathrm{Hom}((\mathbf{Z}/M\mathbf{Z})^\times, \mathbf{U}), \end{array} \tag{6}$$

where δ is the map induced by $(v_D)_*$, the horizontal arrows represent the canonical injections (2), and ${}^t\delta'$ is the transpose of the homomorphism

$\delta' : (\mathbf{Z}/M\mathbf{Z})^\times \to (\mathbf{Z}/N\mathbf{Z})^\times$ *defined in the following way: we write* $N = N_1N_2$ *with* N_2 *the greatest divisor of* N *prime to* M*; if* d *is an integer prime to* M*, then* $\delta'(d+M\mathbf{Z})$ *is the class of the integers congruent to* 1 mod N_2 *and to* $d^{[\Gamma_0(M):\Gamma_0(N)]}$ mod N_1.

REMARK. — Theorems 4 and 5 imply that the map $\beta : \Sigma(M) \to \Sigma(N)$ induced by ${v_D}^*$ and the map $\delta : \Sigma(N) \to \Sigma(M)$ induced by $(v_D)_*$ are independent of the divisor D of N/M.

To each prime number p is associated a *Hecke correspondence* T_p on $X_0(N)$. If $[\tau]$ denotes the image in $X_0(N)$ of an element τ of $\overline{\mathcal{H}}$, then T_p is defined by

$$[\tau] \mapsto [p\tau] + \sum_{0\le i\le p-1} \left[\frac{\tau+i}{p}\right] \qquad \text{if } p \nmid N,$$

$$[\tau] \mapsto \sum_{0\le i\le p-1} \left[\frac{\tau+i}{p}\right] \qquad \text{if } p|N.$$

To these correspondences are associated (by suitably generalising Picard and Albanese functorialities) endomorphisms ${T_p}^*$ and $(T_p)_*$ of $J_0(N)$: for the precise definitions, see §7. One has ${T_p}^* = (T_p)_*$ when $p \nmid N$, but not necessarily so when $p|N$.

THEOREM 6 .— *Both the endomorphisms* ${T_p}^*$ *and* $(T_p)_*$ *stabilise the Shimura subgroup* $\Sigma(N)$ *of* $J_0(N)$ *and, on* $\Sigma(N)$*, they coincide with multiplication by* $p+1$ *if* $p \nmid N$*, and with multiplication by* p *if* $p|N$.

REMARKS.— 1) Theorem 6 was first proved by B. Mazur when N is a prime not equal to p ([3], II, 11.7), then by K. Ribet when p does not divide N([5], thm. 1). For p not dividing eN, where e is the exponent of $\Sigma(N)$, thm. 6 could also be deduced from thm. 2 by using the Eichler-Shimura congruences (see [3], p.89).

2) Theorem 6 can be generalised to the Hecke correspondences T_n, where $n \ge 1$ is not necessarily a prime (see §7): then ${T_n}^*$ and $(T_n)_*$ coincide on $\Sigma(N)$ with multiplication by $a_N(n)$, where $a_N(n)$ denotes the sum of the divisors d of n satisfying the condition $\gcd(N, \frac{n}{d}) = 1$.

1 Some results on Riemann surfaces and their Jacobian varieties

Let X be a compact connected non-empty Riemann surface.

1.1 The Jacobian variety

We shall view the Jacobian variety $J(X)$ of X as the connected component of 0 in the Picard variety of X: it parametrises the isomorphism classes of holomorphic line bundles of degree 0 on X.

1.2 The Albanese variety

The Albanese variety $\mathrm{Alb}(X)$ of X parametrises the classes, modulo principal divisors, of divisors of degree 0 on X. We have a canonical isomorphism $J(X) \to \mathrm{Alb}(X)$: to the class of a holomorphic line bundle of degree 0 corresponds the class of the divisors of its meromorphic sections.

1.3 The group isomorphism $J(X) \to \mathbf{Hom}(H_1(X, \mathbf{Z}), \mathbf{U})$

Let $\mathbf{U}$ be the group of complex numbers of modulus 1 and let $\underline{\mathbf{U}}$ be the sheaf on X of locally constant functions with values in $\mathbf{U}$. The group homomorphism $H^1(X, \underline{\mathbf{U}}) \to H^1(X, \mathcal{O}_X^\times)$ deduced from the injection $\underline{\mathbf{U}} \to \mathcal{O}_X^\times$ defines, when $H^1(X, \mathcal{O}_X^\times)$ is identified with the Picard group of X, a group isomorphism

$$H^1(X, \underline{\mathbf{U}}) \longrightarrow J(X). \tag{7}$$

(This is proved by comparing the exact sequences in Čech cohomology associated to $0 \to \underline{\mathbf{Z}} \to \underline{\mathbf{R}} \to \underline{\mathbf{U}} \to 0$ and $0 \to \underline{\mathbf{Z}} \to \mathcal{O}_X \to \mathcal{O}_X^\times \to 0$; see [4], p.316-05)

We can restate this result as follows:

PROPOSITION 1 .— *Let L be a holomorphic line bundle of degree 0 on X. There exists a principal covering E of the topological space X, with structure group $\mathbf{U}$ (viewed as a discrete group), such that L is isomorphic to the associated holomorphic line bundle $E \times_{\mathbf{U}} \mathbf{C}$. Furthermore, L determines E up to isomorphism.*

We recall that $E \times_{\mathbf{U}} \mathbf{C}$ denotes the quotient of $E \times \mathbf{C}$ by the equivalence relation which identifies $(y, \lambda\mu)$ with $(y\lambda, \mu)$ for $y \in E$, $\lambda \in \mathbf{U}$, $\mu \in \mathbf{C}$. The image of (y, μ) in $E \times_{\mathbf{U}} \mathbf{C}$ will be denoted by $[y, \mu]$.

Let $H_1(X, \mathbf{Z})$ be the first singular homology group of X with coefficients in $\mathbf{Z}$. We shall now deduce from (7) a canonical group isomorphism

$$\phi : J(X) \longrightarrow \mathrm{Hom}(H_1(X, \mathbf{Z}), \mathbf{U}). \tag{8}$$

Let L be a holomorphic line bundle of degree 0 on X and $[L]$ its class in $J(X)$. Let E be as in prop. 1, and let x be a point of X. Since $\pi_1(X,x)^{\mathrm{ab}}$ is canonically isomorphic to $H_1(X,\mathbf{Z})$, the monodromy map $\pi_1(X,x) \to \mathbf{U}$ of the principal covering E factorises through a homomorphism $H_1(X,\mathbf{Z}) \to \mathbf{U}$. This homomorphism depends only on $[L]$ and is, by definition, $\phi([L])$. The fact that ϕ is an isomorphism is seen by combining isomorphism (7) with the comparison between Čech cohomology and singular cohomology. (Remark: In fact, ϕ is an isomorphism of real Lie groups.)

We shall now give an explicit description of the group isomorphism

$$\phi' : \mathrm{Alb}(X) \longrightarrow \mathrm{Hom}(H_1(X,\mathbf{Z}),\mathbf{U}) \tag{9}$$

obtained by composing ϕ with the canonical isomorphism $\mathrm{Alb}(X) \to J(X)$ (see 1.2).

PROPOSITION 2 .— *Let $D = \sum n_i P_i$ be a divisor of degree 0 on X. There exists a unique meromorphic differential form ω_D on X satisfying the two following conditions:*

(i) The only poles of ω_D are simple poles at the points P_i, with residues n_i;

(ii) For each singular 1-cycle c on X, with support disjoint from the support of D, the real part of $\int_c \omega_D$ is 0.

Let $[D]$ denote the class of D in $\mathrm{Alb}(X)$, and for c as in (ii), let $[c]$ denote the class of c in $H_1(X,\mathbf{Z})$. We then have

$$\phi'([D])([c]) = \exp(-\int_c \omega_D). \tag{10}$$

The existence of a meromorphic differential form on X satisfying condition (i) is a consequence of Riemann-Roch theorem. Such a form is unique up to addition of a holomorphic differential form on X, and the $\mathbf{R}$-linear map $H^0(X,\Omega^1) \to \mathrm{Hom}(H_1(X,\mathbf{Z}),\mathbf{R})$ defined by $\omega \mapsto ([c] \mapsto \mathrm{Re}(\int_c \omega))$ is known to be bijective. This establishes the existence and the uniqueness of ω_D.

We consider now a holomorphic line bundle L of degree 0 on X having a meromorphic section s with divisor D. Let E be as in prop. 1. We identify L with $E \times_{\mathbf{U}} \mathbf{C}$. We define a meromorphic differential form ω on X as follows: locally, s can be written as $[h,f]$, with h a continuous section of E and f a meromorphic function, and ω is given by $\omega = df/f$. The form

ω satisfies condition (i) of prop. 2. Let c be a singular 1-cycle on X with support disjoint from the support of D. We shall prove the equality

$$\phi([L])([c]) = \exp(-\int_c \omega). \tag{11}$$

It implies that ω satisfies condition (ii) of prop. 2, hence is equal to ω_D, and (10) follows because $[L]$ corresponds to $[D]$ by the canonical isomorphism $J(X) \to \mathrm{Alb}(X)$. By the residue theorem, the right hand side of (11) depends only on the homology class $[c]$ of c, and it is sufficient to prove (11) when c is a smooth loop. Let $\tilde{c} : [0,1] \to E$ be a path which lifts c. By definition, $\phi([L])([c])$ is the complex number $\lambda \in \mathbf{U}$ such that $\tilde{c}(1) = \tilde{c}(0)\lambda$. We can write $s \circ c$ as $t \mapsto [\tilde{c}(t), f(t)]$ with $f : [0,1] \to \mathbf{C}$ a smooth function and we have, by definition of ω,

$$\exp(-\int_c \omega) = \exp(-\int_0^1 \frac{f'}{f}(t)dt) = \frac{f(0)}{f(1)}.$$

Finally, the equalities $[\tilde{c}(0), f(0)] = s(c(0)) = s(c(1)) = [\tilde{c}(1), f(1)] = [\tilde{c}(0)\lambda, f(1)] = [\tilde{c}(0), \lambda f(1)]$ imply $f(0) = \lambda f(1)$ and this completes the proof.

1.4 Picard and Albanese functorialities

Let Y be a second compact connected Riemann surface, let $f : X \to Y$ be a non-constant holomorphic map and let n be its degree.

To f are associated two morphisms of abelian varieties

$$f^* : \mathrm{Alb}(Y) \to \mathrm{Alb}(X) \quad \text{and} \quad f_* : \mathrm{Alb}(X) \to \mathrm{Alb}(Y).$$

The morphism f^* sends the class of a divisor of degree 0 on Y to the class of its inverse image under f; the morphism f_* sends the class of a divisor of degree 0 on X to the class of its image under f. The map $f_* \circ f^*$ coincides with multiplication by n in $\mathrm{Alb}(Y)$. The kernel of f^* is therefore finite.

Via the canonical isomorphisms between Albanese and Jacobian varieties (see 1.2), we can view the previous maps as morphisms of abelian varieties

$$f^* : J(Y) \to J(X) \quad \text{and} \quad f_* : J(X) \to J(Y).$$

The morphism f^* sends the class of a line bundle L of degree 0 on Y to the class of its pullback $X \times_Y L$. The morphism f_* sends the class of a

line bundle L' of degree 0 on X to the class of its norm $N_{X/Y}L'$ (for the definition of this line bundle in the language of invertible sheaves, see [1], 6.5); this description of f_* will not be used in this paper. We shall say that f^* is deduced from f by Picard functoriality and that f_* is deduced from f by Albanese functoriality.

By taking images by f and inverse images by f of singular 1-cycles, one also defines two group homomorphisms

$$f_* : H_1(X, \mathbf{Z}) \to H_1(Y, \mathbf{Z}) \quad \text{and} \quad f^* : H_1(Y, \mathbf{Z}) \to H_1(X, \mathbf{Z}).$$

We claim that the two diagrams

$$\begin{array}{ccc} J(Y) & \longrightarrow & \mathrm{Hom}(H_1(Y, \mathbf{Z}), \mathbf{U}) \\ f^* \downarrow & & \downarrow {}^t f_* \\ J(X) & \longrightarrow & \mathrm{Hom}(H_1(X, \mathbf{Z}), \mathbf{U}) \end{array} \tag{12}$$

and

$$\begin{array}{ccc} J(X) & \longrightarrow & \mathrm{Hom}(H_1(X, \mathbf{Z}), \mathbf{U}) \\ f_* \downarrow & & \downarrow {}^t f^* \\ J(Y) & \longrightarrow & \mathrm{Hom}(H_1(Y, \mathbf{Z}), \mathbf{U}), \end{array} \tag{13}$$

where the horizontal arrows represent the canonical isomorphisms (8), are commutative. The commutativity of (12) follows immediately from the definitions. The commutativity of (13) is seen more easily by considering Albanese varieties. Let D be a divisor of degree 0 on X and ω_D the corresponding meromorphic differential form (see prop. 2). The trace $\omega = Tr_{X/Y}(\omega_D)$ of ω_D is a meromorphic differential form on Y; it satisfies condition (i) of prop. 2 with respect to the image $f(D)$ of the divisor D on Y, and we have $\int_c \omega = \int_{f^{-1}c} \omega_D$ for each singular 1-cycle c on Y, with support disjoint from the support of $f(D)$. This first implies that ω is equal to $\omega_{f(D)}$ and then implies the commutativity of (13) by formula (10).

REMARK.— Let $g : Z \to Y$ be the maximal abelian unramified covering of the Riemann surface Y through which f factorises, and let A denote its Galois group. Let x be a point of X. By monodromy, A is isomorphic to the largest abelian quotient of $\pi_1(Y, f(x))$ to which $\pi_1(X, x)$ maps to 0, i.e., A is isomorphic to the cokernel of $f_* : H_1(X, \mathbf{Z}) \to H_1(Y, \mathbf{Z})$. This latter isomorphism does not depend on x. We deduce from it, by using the commutative diagram (12), a canonical isomorphism $\eta : \Sigma \to \mathrm{Hom}(A, \mathbf{U})$, where Σ denotes the kernel of $f^* : J(Y) \to J(X)$. If χ is an element of

$\mathrm{Hom}(A, \mathbf{U})$, $\eta^{-1}(\chi)$ is described explicitly as follows: it is the isomorphism class of the line bundle $Z \times_A \mathbf{C}$ associated to the covering Z and to the action $(a, \lambda) \mapsto \chi(a)\lambda$ of A on $\mathbf{C}$.

1.5 The case of modular curves

Let Γ be a subgroup of $SL_2(\mathbf{Z})$ of finite index. Let X denote the Riemann surface $\Gamma\backslash\overline{\mathcal{H}}$ and $p : \overline{\mathcal{H}} \to X$ the canonical surjection. For each point $\tau \in \overline{\mathcal{H}}$, there is a group homomorphism

$$\Gamma \longrightarrow \pi_1(X, p(\tau)) \tag{14}$$

characterised by the following property: if γ is an element of Γ and c a continuous path in $\overline{\mathcal{H}}$ connecting τ to $\gamma\tau$, the image of γ by the homomorphism (14) is the (strict) homotopy class of the loop $p \circ c$. The homomorphism (14) is surjective and its kernel is the subgroup of Γ generated by the elements fixing at least one point in $\overline{\mathcal{H}}$, i.e., those whose trace t satisfies $|t| \leq 2$ ([7], p.5). Since $\pi_1(X, p(\tau))^{\mathrm{ab}}$ is canonically isomorphic to $H_1(X, \mathbf{Z})$, we deduce from (14) a surjective homomorphism

$$\Gamma \longrightarrow H_1(X, \mathbf{Z}). \tag{15}$$

This homomorphism does not depend on τ.

Let $J(X)$ denote the Jacobian variety of X. By composing the transpose of the isomorphism (15) with the isomorphism (8) of 1.3, we get a canonical injective group homomorphism

$$\psi_\Gamma : J(X) \longrightarrow \mathrm{Hom}(\Gamma, \mathbf{U}). \tag{16}$$

A homomorphism $\Gamma \to \mathbf{U}$ belongs to the image of ψ_Γ if and only if its kernel contains the elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ such that $|a + d| \leq 2$.

Let Γ' be a second subgroup of $SL_2(\mathbf{Z})$ of finite index and X' the Riemann surface $\Gamma'\backslash\overline{\mathcal{H}}$. We first assume that there exists a matrix $g \in GL_2^+(\mathbf{R})$ such that $g\Gamma' g^{-1} \subseteq \Gamma$. Let g be such a matrix. By passing to the quotients, we deduce from the transformation $\tau \mapsto g\tau$ of $\overline{\mathcal{H}}$ a holomorphic map $w : X' \to X$ and hence, by Picard functoriality, a morphism $w^* : J(X) \to J(X')$ of abelian varieties. Let $v : \Gamma' \to \Gamma$ denote the homomorphism $\gamma \mapsto g\gamma g^{-1}$ from Γ' to Γ.

PROPOSITION 3 .— *The diagram*

$$\begin{array}{ccc} J(X) & \xrightarrow{\psi_\Gamma} & \mathrm{Hom}(\Gamma, \mathbf{U}) \\ {\scriptstyle w^*}\downarrow & & \downarrow {\scriptstyle {}^t v} \\ J(X') & \xrightarrow{\psi_{\Gamma'}} & \mathrm{Hom}(\Gamma', \mathbf{U}) \end{array}$$

is commutative.

This follows from the commutativity of the diagram (12) and that of the diagram

$$\begin{array}{ccc} \Gamma' & \longrightarrow & H_1(X', \mathbf{Z}) \\ {\scriptstyle v}\downarrow & & \downarrow {\scriptstyle w_*} \\ \Gamma & \longrightarrow & H_1(X, \mathbf{Z}). \end{array}$$

We now assume that Γ' is contained in Γ. We denote by $u : X' \to X$ the holomorphic map deduced from the identity on $\overline{\mathcal{H}}$ by passing to the quotients, and by $u_* : J(X') \to J(X)$ the morphism of abelian varieties deduced from u by Albanese functoriality. Since Γ' is of finite index in Γ, we have a transfer homomorphism (see [2], p.202)

$$V : \Gamma^{\mathrm{ab}} \longrightarrow \Gamma'^{\mathrm{ab}}.$$

We recall its definition: if $S \subseteq \Gamma$ is a system of representatives of $\Gamma' \backslash \Gamma$, and if γ is an element of Γ, there exist a permutation σ of S and, for each $s \in S$, an element $a_{s,\gamma}$ of Γ' such that $s\gamma = a_{s,\gamma}\sigma(s)$. Let $\overline{\gamma}$ denote the image of γ in Γ^{ab} and $\overline{a_{s,\gamma}}$ the image of $a_{s,\gamma}$ in Γ'^{ab}. The product $\prod_{s \in S} \overline{a_{s,\gamma}}$ depends only on $\overline{\gamma}$ (and not on the choice of the system of representatives S) and is equal to $V(\overline{\gamma})$.

PROPOSITION 4 .— *The diagram*

$$\begin{array}{ccccc} J(X') & \xrightarrow{\psi_{\Gamma'}} & \mathrm{Hom}(\Gamma', \mathbf{U}) & = & \mathrm{Hom}(\Gamma'^{\mathrm{ab}}, \mathbf{U}) \\ {\scriptstyle u_*}\downarrow & & & & \downarrow {\scriptstyle {}^t V} \\ J(X) & \xrightarrow{\psi_\Gamma} & \mathrm{Hom}(\Gamma, \mathbf{U}) & = & \mathrm{Hom}(\Gamma^{\mathrm{ab}}, \mathbf{U}) \end{array}$$

is commutative.

We shall prove that the diagram

$$\begin{array}{ccc} \Gamma^{ab} & \xrightarrow{\eta} & H_1(X, \mathbf{Z}) \\ V \downarrow & & \downarrow u^* \\ \Gamma'^{ab} & \xrightarrow{\eta'} & H_1(X', \mathbf{Z}), \end{array} \tag{17}$$

where η, η' are deduced from (15) by passing to the quotients, is commutative. Prop. 4 will then follow from the commutativity of the diagram (13) of 1.4. Let γ be an element of Γ and let $\overline{\gamma}$, S, σ, $a_{s,\gamma}$ and $\overline{a_{s,\gamma}}$ be as introduced before prop. 4. Let τ be a point in $\overline{\mathcal{H}}$, c a continuous path in $\overline{\mathcal{H}}$ connecting τ to $\gamma\tau$ and $q : \overline{\mathcal{H}} \to X'$ the canonical surjection. For each $s \in S$, let c_s be a continuous path in $\overline{\mathcal{H}}$ connecting τ to $s\tau$. By definition of η and u^*, we have

$$u^*(\eta(\overline{\gamma})) = \sum_{s \in S} [q \circ (sc)],$$

where sc denotes the path $t \mapsto sc(t)$ in $\overline{\mathcal{H}}$. As σ is a permutation of S, we can write

$$u^*(\eta(\overline{\gamma})) = \sum_{s \in S} ([q \circ c_s] + [q \circ (sc)] - [q \circ (c_{\sigma(s)})]).$$

We have $q \circ c_{\sigma(s)} = q \circ (a_{s,\gamma} c_{\sigma(s)})$ and the path composed of c_s, of sc and of the inverse of the path $a_{s,\gamma} c_{\sigma(s)}$ connects τ to $a_{s,\gamma}\tau$; we have, therefore,

$$[q \circ (c_s)] + [q \circ (sc)] - [q \circ (c_{\sigma(s)})] = \eta'(\overline{a_{s,\gamma}})$$

in $H_1(X', \mathbf{Z})$ for each $s \in S$, and

$$u^*(\eta(\overline{\gamma})) = \sum_{s \in S} \eta'(\overline{a}_{s,\gamma}) = \eta'(V(\overline{\gamma})).$$

This proves the commutativity of (17).

2 The group structure of $\Sigma(N)$

2.1 The holomorphic map $u : X_1(N) \longrightarrow X_0(N)$

As in the introduction, $u : X_1(N) \to X_0(N)$ denotes the holomorphic map deduced from the identity on $\overline{\mathcal{H}}$ by passing to the quotients.

The group $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$. Therefore, one deduces from the action of $\Gamma_0(N)$ on $\overline{\mathcal{H}}$ an action of $\Gamma_0(N)$ on $X_1(N)$. The group

$\Gamma_1(N)$ and the matrix -1 act trivially on $X_1(N)$, hence we have an action of the group

$$G = \Gamma_0(N)/\{-1,1\}\Gamma_1(N) \simeq (\mathbf{Z}/N\mathbf{Z})^\times/\{-1,1\}$$

on $X_1(N)$. The holomorphic map $u : X_1(N) \to X_0(N)$ is a Galois ramified covering with Galois group G.

REMARK (Modular interpretation).— The Riemann surface $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ parametrises the isomorphism classes of pairs (E, C), where E is an elliptic curve over $\mathbf{C}$ and C a cyclic subgroup of E of order N: to the class mod $\Gamma_0(N)$ of a point $\tau \in \mathcal{H}$ corresponds the class of the pair (E_τ, C_τ), where $E_\tau = \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$ and C_τ is the subgroup of E_τ generated by the image of $\frac{1}{N}$. Similarly, $Y_1(N) = \Gamma_1(N)\backslash\mathcal{H}$ parametrises the isomorphism classes of pairs (E, P), where E is an elliptic curve over $\mathbf{C}$ and P a point of E of exact order N: to the class mod $\Gamma_1(N)$ of a point $\tau \in \mathcal{H}$ corresponds the class of the pair (E_τ, P_τ), where $E_\tau = \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau)$ and P_τ is the image of $\frac{1}{N}$ in E_τ. The map $Y_1(N) \to Y_0(N)$ induced by u has the following modular interpretation: it sends the class $[E, P]$ to the class $[E, \langle P\rangle]$, where $\langle P\rangle$ is the cyclic subgroup of E generated by P. The action of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ on $X_1(N)$ induces on $Y_1(N)$ the transformation given in modular terms by $[E, P] \mapsto [E, dP]$. (Note that the class $[E, -P]$ is always equal to the class $[E, P]$.) This modular interpretation of the action of G explains why we prefer to identify $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$ by using d instead of a.

2.2 Proof of theorem 1

We have defined in 1.5, formula (16), a canonical injective group homomorphism

$$\psi : J_0(N) \longrightarrow \mathrm{Hom}(\Gamma_0(N), \mathbf{U}). \tag{18}$$

Prop. 3, applied with $\Gamma = \Gamma_0(N)$, $\Gamma' = \Gamma_1(N)$ and $g = 1$ implies that an element $x \in J_0(N)$ belongs to the Shimura subgroup $\Sigma(N)$ if and only if the kernel of $\psi(x)$ contains $\Gamma_1(N)$. By identifying $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$, we therefore deduce from ψ a canonical injective homomorphism

$$\psi' : \Sigma(N) \longrightarrow \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}). \tag{19}$$

A homomorphism $h : \Gamma_0(N) \to \mathbf{U}$ belongs to the image of ψ if and only if its kernel contains the set $S = \{\gamma \in \Gamma_0(N) | |Tr(\gamma)| \leq 2\}$ (see 1.5). This set consists of the matrices of the form $\begin{pmatrix} t-d & b \\ Nc & d \end{pmatrix}$, with b, c, d in $\mathbf{Z}$, $t \in \{-2, -1, 0, 1, 2\}$ and $d(t-d) - Nbc = 1$. Its image S' under the canonical surjection $\Gamma_0(N) \to (\mathbf{Z}/N\mathbf{Z})^\times$ ($\simeq \Gamma_0(N)/\Gamma_1(N)$) consists of the roots in $\mathbf{Z}/N\mathbf{Z}$ of the polynomials $X^2 - tX + 1$, for $t \in \{-2, -1, 0, 1, 2\}$. A homomorphism $g : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{U}$ belongs to the image of ψ' if and only if its kernel contains S'. Since -1 belongs to S' and since the roots of $X^2 - tX + 1$ and $X^2 + tX + 1$ are interchanged by multiplication by -1, thm. 1 follows.

2.3 Group structure of $\Sigma(N)$

Let J denote the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by -1 and the roots in $\mathbf{Z}/N\mathbf{Z}$ of the polynomials X^2+1, X^2+X+1 and $(X-1)^2$. The dual of the finite abelian group $\Sigma(N)$ is canonically isomorphic to $(\mathbf{Z}/N\mathbf{Z})^\times/J$ (thm. 1). We shall describe explicitly the latter group in this section. First, we recall some notations introduced in cor. 1 of thm. 1:

(i) Let m denote the largest integer such that m^2 divides N.

(ii) Let m_2 be equal to 2 if -1 is a square mod N (i.e., if $4 \nmid N$ and each prime factor $p \neq 2$ of N is congruent to 1 mod 4), and let m_2 be equal to 1 otherwise.

(iii) Let m_3 be equal to 3 if $X^2 + X + 1$ has a root mod N (i.e., if $9 \nmid N$ and each prime factor $p \neq 3$ of N is congruent to 1 mod 3), and let m_3 be equal to 1 otherwise.

LEMMA 1 .— *The set of roots of $(X-1)^2$ in $\mathbf{Z}/N\mathbf{Z}$ is the kernel of the canonical surjection $(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/(N/m)\mathbf{Z})^\times$; it is contained in J.*

By the definition of m, an element of $\mathbf{Z}/N\mathbf{Z}$ has square 0 if and only if it is congruent to 0 mod N/m. This proves the first assertion. The second assertion follows from the definition of J.

Let J' denote the image of J in $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$. By lemma 1, the canonical map

$$(\mathbf{Z}/N\mathbf{Z})^\times/J \longrightarrow (\mathbf{Z}/(N/m)\mathbf{Z})^\times/J' \tag{20}$$

is bijective.

If p is an odd prime and $r \geq 1$ is an integer, the group $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is canonically isomorphic to $\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r-1}\mathbf{Z})$ (the class of $1+p$ mod $p^r\mathbf{Z}$ corresponds to $(1, 1+p^{r-1}\mathbf{Z})$). Let $N = \prod p^{r_p}$ be the prime power decomposition of N. By the Chinese remainder theorem, we get an isomorphism

$$(\mathbf{Z}/(N/m)\mathbf{Z})^\times \simeq (\mathbf{Z}/2^{r_2-[r_2/2]}\mathbf{Z})^\times \times \prod_{p|N, p\neq 2} (\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r'_p}\mathbf{Z})), \qquad (21)$$

where, for each prime factor $p \neq 2$ of N, r'_p denotes the integer $r_p - [r_p/2] - 1$. If a prime p distinct from 2 and 3 divides N, we have that $p \equiv 1$ mod $2m_2m_3$ by definition of m_2 and m_3, and the group $\mu_{m_2m_3}(\mathbf{F}_p)$ of m_2m_3-th roots of unity in $\mathbf{F}_p$ has order m_2m_3. We shall denote by J'' the subgroup of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ corresponding to $\prod_{p|N, p\notin\{2,3\}} \mu_{m_2m_3}(\mathbf{F}_p)$ via the isomorphism (21).

PROPOSITION 5 .— *Assume that N is different from $1, 2$ and 4. The group J'' is a subgroup of index 2 of J'. If -1 is not a square* mod N, *then -1 belongs to $J' - J''$. If -1 is a square* mod N, *then any square root of -1 in $\mathbf{Z}/N\mathbf{Z}$ reduces modulo N/m to an element of $J' - J''$.*

By lemma 1, the group J' is the image under the canonical surjection $(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/(N/m)\mathbf{Z})^\times$ of the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by -1 and the roots of X^2+1 and X^2+X+1.

As we have $N \neq 1, 2, 4$ by hypothesis, we have $N/m \geq 3$, and $-1 \neq 1$ in $\mathbf{Z}/(N/m)\mathbf{Z}$. This implies the two last assertions of prop. 5 because every element x of J'' satisfies $x^3 = 1$ when -1 is not a square mod N and satisfies $x^6 = 1$ when -1 is a square mod N.

Let $\mu_2(\mathbf{Z}/N\mathbf{Z})$ and $\mu_3(\mathbf{Z}/N\mathbf{Z})$ denote the groups of square roots and third roots of unity in $\mathbf{Z}/N\mathbf{Z}$ respectively. The proposition is now a consequence of the following two lemmas.

LEMMA 2 .— *Assume that there exists $a \in \mathbf{Z}/N\mathbf{Z}$ such that $a^2 + 1 = 0$. The subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by the roots of X^2+1 is equal to $\mu_2(\mathbf{Z}/N\mathbf{Z}) \cup \mu_2(\mathbf{Z}/N\mathbf{Z})a$; it contains -1. The reduction modulo N/m of $\mu_2(\mathbf{Z}/N\mathbf{Z})$ is the 2-torsion subgroup of J''.*

The roots of X^2+1 in $\mathbf{Z}/N\mathbf{Z}$ are the elements of $\mu_2(\mathbf{Z}/N\mathbf{Z})a$, and $a^2 = -1$ belongs to $\mu_2(\mathbf{Z}/N\mathbf{Z})$. This implies our first assertion. The existence of a square root of -1 mod N implies that N is divisible by neither 3 nor 4. The last assertion follows easily.

LEMMA 3 .— *Assume that X^2+X+1 has a root in $\mathbf{Z}/N\mathbf{Z}$. The subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by these roots is then equal to $\mu_3(\mathbf{Z}/N\mathbf{Z})$ and its reduction modulo N/m is the 3-torsion subgroup of J''.*

Our hypothesis implies that N is divisible by neither 2 nor 9; we may write N as N' or $3N'$, with N' prime to 6. When identifying $(\mathbf{Z}/N\mathbf{Z})^\times$ with $\prod_{p|N}(\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r_p-1}\mathbf{Z}))$, the group $\mu_3(\mathbf{Z}/N\mathbf{Z})$ gets identified with $\prod_{p|N'}\mu_3(\mathbf{F}_p)$. The last assertion of the lemma follows. All roots of X^2+X+1 in $\mathbf{Z}/N\mathbf{Z}$ belong to $\mu_3(\mathbf{Z}/N\mathbf{Z})$. The group $\mu_3(\mathbf{Z}/N\mathbf{Z})$ is generated by the elements x such that $x \not\equiv 1 \bmod p$ for each prime divisor p of N'. For such an x, the relation $(x-1)(x^2+x+1) = x^3-1 = 0$ implies that $x^2+x+1 \equiv 0 \bmod N'$; furthermore, if 3 divides N, we have that $x \equiv 1 \bmod 3$ and hence $x^2+x+1 \equiv 1+1+1 \equiv 0 \bmod 3$. This shows that x is a root of X^2+X+1 in $\mathbf{Z}/N\mathbf{Z}$, and hence completes the proof.

The finite abelian group $\Sigma(N)$ is (non-canonically) isomorphic to its dual $(\mathbf{Z}/N\mathbf{Z})^\times/J$ and hence to $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/J'$ (see (20)). From the explicit description of J' given in prop. 5, and from (21), we deduce:

COROLLARY 1 .— *Assume that -1 is a square* mod N *and that $N \neq 1, 2$. Then N is of the form N' or $2N'$, with $N' \neq 1$ and each prime factor of N' congruent to* 1 mod $4m_3$. *The group $\Sigma(N)$ is isomorphic to the quotient of the group*

$$\prod_{p|N'}((\mathbf{Z}/\tfrac{p-1}{2m_3}\mathbf{Z}) \times (\mathbf{Z}/p^{r'_p}\mathbf{Z}))$$

by the unique subgroup of order 2 which has a non-zero projection on each factor $\mathbf{Z}/\frac{p-1}{2m_3}\mathbf{Z}$.

COROLLARY 2 .— *Assume that -1 is not a square* mod N. *Then the group $\Sigma(N)$ is isomorphic to $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/(\{-1,1\}\mu_{m_3}(\mathbf{Z}/(N/m)\mathbf{Z}))$.*

3 The order and the exponent of $\Sigma(N)$

In this section, the symbols $m, k, m_1, m_2, m_3, e_0, r_p$ and r'_p have the same meaning as in cor. 1 and cor. 2 of thm. 1.

3.1 The order of $\Sigma(N)$

If $N \leq 4$, the group $(\mathbf{Z}/N\mathbf{Z})^\times/\{-1,1\}$ has order 1 and hence $\Sigma(N)$ has order 1 (thm. 1).

Assume now that $N \geq 5$. In 2.3, we have defined an isomorphism between the dual of the finite abelian group $\Sigma(N)$ and the quotient of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ by a certain subgroup J'. Since m^2 divides N, the order of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ is $\phi(N)/m$, where ϕ denotes the Euler function. We have shown in prop. 5 that J' has a subgroup of index 2 which is of order $m_2^k m_3^k$. In conclusion, we have (for $N \geq 5$)

$$\operatorname{Card}\Sigma(N) = \phi(N)/(2mm_2^k m_3^k).$$

This proves cor. 1 of thm. 1.

3.2 The exponent of $\Sigma(N)$

Let e be the exponent of $\Sigma(N)$. If $N \leq 4$, then $\Sigma(N)$ has order 1 and we have $e = 1$. From now on, we assume that $N \geq 5$. We shall prove cor. 2 of thm. 1 by distinguishing between two cases:

a) *The case where* -1 *is a square* mod N *(i.e.,* $m_2 = 2$*)*

In this case, N is of the form N' or $2N'$, with $N' \neq 1$ and each prime factor of N' congruent to 1 mod $4m_3$, and $\Sigma(N)$ is isomorphic to the quotient of the group

$$A = \prod_{p|N'} ((\mathbf{Z}/\tfrac{p-1}{2m_3}\mathbf{Z}) \times (\mathbf{Z}/p^{r'_p}\mathbf{Z}))$$

by the unique subgroup of order 2 which has a non-zero projection on each factor $\mathbf{Z}/\frac{p-1}{2m_3}\mathbf{Z}$ (2.3, cor. 1 of prop. 5). The exponent of $\Sigma(N)$ is the same as that of A if N' has at least two prime divisors (i.e., if $m_1 = 1$), and is equal to that of A divided by 2 if N' has only one prime divisor (i.e., if $m_1 = 2$). As the exponent e_A of A is given by

$$e_A = \operatorname*{lcm}_{p|N'}\left(\frac{p-1}{2m_3}p^{r'_p}\right) = \frac{1}{2m_3}\operatorname*{lcm}_{p|N'}((p-1)p^{r'_p}) = \frac{e_0}{2m_3},$$

we have

$$e = e_A/m_1 = e_0/2m_1m_3 = e_0/m_1m_2m_3.$$

b) *The case where* -1 *is not a square* mod N *(i.e.,* $m_2 = 1$*)*

In this case, the group $\Sigma(N)$ is isomorphic to the quotient group $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/(\{-1,1\}\mu_{m_3}(\mathbf{Z}/(N/m)\mathbf{Z}))$ (2.3, cor. 2 of prop. 5). Its exponent e is equal to the exponent e' of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/\{-1,1\}$ divided by m_3.

We first assume that $r_2 \leq 2$. Then $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ is isomorphic to $\prod_{p|N,p\neq 2}(\mathbf{F}_p^\times \times (\mathbf{Z}/p^{r'_p}\mathbf{Z}))$ and the exponent of $(\mathbf{Z}/(N/m)\mathbf{Z})^\times$ is

$$\operatorname*{lcm}_{p|N,p\neq 2}((p-1)p^{r'_p}) = \operatorname*{lcm}_{p|N}((p-1)p^{r'_p}) = e_0.$$

The integer N has at least one odd prime divisor because we have assumed that $N \geq 5$; we have $e' = e_0$ if N has at least two such divisors (i.e., if $m_1 = 1$) and $e' = e_0/2$ if it has only one such divisor (i.e., if $m_1 = 2$). In conclusion, we have

$$e = e'/m_3 = e_0/m_1m_3 = e_0/m_1m_2m_3.$$

We now assume that $r_2 \geq 3$ (hence $m_1 = 1$). We have then an isomorphism (see 2.3, (21))

$$(\mathbf{Z}/(N/m)\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{r'_2}\mathbf{Z} \times \prod_{p|N,p\neq 2}(\mathbf{F}_p^\times \times \mathbf{Z}/p^{r'_p}\mathbf{Z})$$

such that the projection of -1 on the factor $\mathbf{Z}/2\mathbf{Z}$ is of order 2. The group $(\mathbf{Z}/(N/m)\mathbf{Z})^\times/\{-1,1\}$ is hence isomorphic to $\mathbf{Z}/2^{r'_2}\mathbf{Z} \times \prod_{p|N,p\neq 2}(\mathbf{F}_p^\times \times \mathbf{Z}/p^{r'_p}\mathbf{Z})$ and its exponent e' is $\operatorname*{lcm}_{p|N}((p-1)p^{r'_p}) = e_0$. In conclusion, we have

$$e = e'/m_3 = e_0/m_3 = e_0/m_1m_2m_3.$$

3.3 Cases where the exponent of $\Sigma(N)$ is 1 or 2

Let $N \geq 1$ be an integer such that the exponent e of $\Sigma(N)$ is 1 or 2.

For each odd prime divisor p of N, the exponent r_p of p in the prime power decomposition of N is at most 2: otherwise, p would divide e (cor. 2 of thm. 1). Furthermore, $p-1$ divides $m_1m_2m_3e$ (*loc. cit.*) and *a fortiori* 24, hence p belongs to the set $\{3,5,7,13\}$.

The integer N cannot be divisible by 2.7, 2.13, 5.7, 5.13 or $3^2.7$ because, in these cases, we have $m_3 = 1$ and $3|e$ (*loc. cit.*). It cannot be divisible by

3.5, 3.13, 7.13, $2^3.5$ or 2^7 because, in these cases, we have $m_1 = m_2 = 1$ and $4|e$ (*loc. cit.*). From this, we deduce:

(a) If N is divisible by 13, it is equal to 13 or 13^2. In both cases, we have, in fact, $e = 1$.

(b) If N is divisible by 7, it is equal to $7, 7^2, 3.7$ or 3.7^2. We have, in fact, $e = 1$ in the first two cases and $e = 2$ in the last two.

(c) If N is divisible by 5, it is equal to $5, 5^2, 2.5, 2.5^2, 2^2.5$ or $2^2.5^2$. We have, in fact, $e = 1$ in the first four cases and $e = 2$ in the last two.

(d) If N is divisible by 3 and not by 7, it is of the form $2^a 3$ or $2^a 3^2$, with $0 \leq a \leq 6$. We have, in fact, $e = 1$ if $a \leq 2$ and $e = 2$ if $3 \leq a \leq 6$.

(e) If N is a power of 2, it is equal to 2^a, with $0 \leq a \leq 6$. We have, in fact, $e = 1$ if $a \leq 4$ and $e = 2$ if $a = 5$ or $a = 6$.

The integers N for which $e = 1$, i.e., for which the group $\Sigma(N)$ has order 1, are therefore $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25, 36, 49, 50$ and 169. This proves cor. 3 of thm. 1.

The integers N for which $e = 2$ are $20, 21, 24, 32, 48, 64, 72, 96, 100, 144, 147, 192, 288$ and 576.

3.4 Behaviour when N approaches infinity

Let S be a set of positive integers such that the exponents of the groups $\Sigma(N)$, for $N \in S$, are bounded. Cor. 2 of thm. 1 shows that the prime divisors of the integers $N \in S$ are bounded, and that for each prime number p, the exponent of p in N, $N \in S$, is bounded. This implies that S is finite.

In other words, when N approaches infinity, so does the exponent of $\Sigma(N)$. This proves cor. 4 of thm. 1.

4 Action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\Sigma(N)$

4.1 The remark of section 1.4 revisited in algebraic geometry

Let K be a field of characteristic 0 and let $\overline{K}$ be an algebraic closure of K. If S is a K-scheme, we denote the $\overline{K}$-scheme $S \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, \overline{K}$ by $S_{\overline{K}}$.

Let X, Y be two absolutely irreducible proper smooth curves over K, and let $f : X \to Y$ be a non-constant morphism (over K). Let $g : Z \to Y$

be the maximal unramified covering of Y through which f factorises, such that $g_{\overline{K}} : Z_{\overline{K}} \to Y_{\overline{K}}$ is an abelian covering; let A denote the Galois group of the covering $g_{\overline{K}}$. For $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $a \in A$, there exists a unique $\sigma(a) \in A$ such that the diagram

$$\begin{array}{ccc} Z_{\overline{K}} & \xrightarrow{1_Z \times \mathrm{Spec}\,\sigma} & Z_{\overline{K}} \\ {\scriptstyle \sigma(a)}\downarrow & & \downarrow{\scriptstyle a} \\ Z_{\overline{K}} & \xrightarrow{1_Z \times \mathrm{Spec}\,\sigma} & Z_{\overline{K}} \end{array} \tag{22}$$

is commutative. This defines an action of $\mathrm{Gal}(\overline{K}/K)$ on A. We deduce an action $(\sigma, \chi) \mapsto {}^{\sigma}\chi$ of $\mathrm{Gal}(\overline{K}/K)$ on the character group $\hat{A} = \mathrm{Hom}(A, \overline{K}^{\times})$ characterised by the formula $({}^{\sigma}\chi)(a) = \sigma(\chi(\sigma^{-1}(a)))$.

Let $J(X)$ and $J(Y)$ be the Jacobian varieties of X and Y, viewed as the connected components of 0 in the Picard varieties. The group $J(X)(\overline{K})$ parametrises the isomorphism classes of line bundles of degree 0 on $X_{\overline{K}}$. We denote by $f^* : J(Y)(\overline{K}) \to J(X)(\overline{K})$ the homomorphism deduced from f by Picard functoriality.

For each $\chi \in \hat{A}$, there is a line bundle L_χ on $Y_{\overline{K}}$ associated to the Galois covering $Z_{\overline{K}} \to Y_{\overline{K}}$; its underlying scheme is $(Z_{\overline{K}} \times_{\mathrm{Spec}\,\overline{K}} \mathbf{A}^1_{\overline{K}})/A$, where A acts simultaneously on $Z_{\overline{K}}$ and on the affine line $\mathbf{A}^1_{\overline{K}}$, the action on $\mathbf{A}^1_{\overline{K}}$ being given by $a \mapsto \chi(a^{-1})$. The pullback of L_χ on $Z_{\overline{K}}$, and *a fortiori* on $X_{\overline{K}}$, is the trivial line bundle, hence L_χ is of degree 0 and its isomorphism class $[L_\chi]$ belongs to the kernel of f^*.

PROPOSITION 6 .— *The map $\chi \mapsto [L_\chi]$ is a group isomorphism from $\hat{A}$ to the kernel of $f^* : J(Y)(\overline{K}) \to J(X)(\overline{K})$, compatible with the actions of* $\mathrm{Gal}(\overline{K}/K)$.

To prove that the map $\chi \mapsto [L_\chi]$ is a group isomorphism, we can assume that K is equal to $\overline{K}$, then reduce to the case where $K = \mathbf{C}$ by the Lefschetz principle, and finally use the GAGA principle to derive the result from the analogous result for compact connected Riemann surfaces (see 1.4, remark).

We shall now prove the compatibility with the actions of Galois. Let σ be an element of $\mathrm{Gal}(\overline{K}/K)$ and let L be a line bundle of degree 0 on $Y_{\overline{K}}$. The $\overline{K}$-scheme ${}^{\sigma}L$ deduced from L by the base change $\mathrm{Spec}\,\sigma$ is a line bundle of degree 0 on $Y_{\overline{K}}$: this is because the $\overline{K}$-scheme deduced from $Y_{\overline{K}}$ by this base change is $Y_{\overline{K}}$. The action of $\mathrm{Gal}(\overline{K}/K)$ on $J(Y)(\overline{K})$ is none other than $(\sigma, [L]) \mapsto [{}^{\sigma}L]$. Now let us consider the case where L is the line bundle $L_\chi = (Z_{\overline{K}} \times_{\mathrm{Spec}\,\overline{K}} \mathbf{A}^1_{\overline{K}})/A$ associated to a character $\chi \in \hat{A}$. Then

${}^{\sigma}L$ is the quotient $(Z_{\overline{K}} \times_{\operatorname{Spec} \overline{K}} \mathbf{A}^1_{\overline{K}})/A$, where A acts on $Z_{\overline{K}}$ by $a \mapsto \sigma(a)$ (see diagram (22)) and acts on $\mathbf{A}^1_{\overline{K}}$ by $a \mapsto \sigma(\chi(a^{-1}))$. This is the same as taking the quotient $(Z_{\overline{K}} \times_{\operatorname{Spec} \overline{K}} \mathbf{A}^1_{\overline{K}})/A$, where the action of A on $Z_{\overline{K}}$ is the original action and where A acts on $\mathbf{A}^1_{\overline{K}}$ by $a \mapsto {}^{\sigma}\chi(a^{-1})$. Hence, we have $[{}^{\sigma}(L_\chi)] = [L_{{}^{\sigma}\chi}]$. This completes the proof.

4.2 Galois action on the Shimura subgroup

The Riemann surfaces $X_1(N)$ and $X_0(N)$ are the sets of complex points of algebraic modular curves naturally defined over $\mathbf{Q}$, denoted by $X_1(N)_{\mathbf{Q}}$ and $X_0(N)_{\mathbf{Q}}$: these may be defined as the smooth compactifications of the coarse moduli schemes associated to the modular problems described in the remark of 2.1 (modular problems which make sense over $\mathbf{Q}$). The holomorphic map $u : X_1(N) \to X_0(N)$ considered in 2.1 comes from a morphism $u_{\mathbf{Q}} : X_1(N)_{\mathbf{Q}} \to X_0(N)_{\mathbf{Q}}$ and each automorphism $g \in G$ (with $G = \Gamma_0(N)/\{-1,1\}\Gamma_1(N) \simeq (\mathbf{Z}/N\mathbf{Z})^\times/\{-1,1\}$) of the covering u comes from an automorphism of $X_1(N)_{\mathbf{Q}}$: this follows from the modular description of u and G (2.1, remark).

We have defined in 2.2 a canonical injective homomorphism

$$\psi' : \Sigma(N) \longrightarrow \operatorname{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U}).$$

Let A denote the Galois group of the maximal abelian unramified covering of $X_0(N)$ through which u factorises. It is a quotient of G, and hence of $(\mathbf{Z}/N\mathbf{Z})^\times$. The homomorphism ψ' is none other than the homomorphism obtained by composing the isomorphism $\Sigma(N) \to \operatorname{Hom}(A, \mathbf{U})$ defined in the remark of 1.4 and the canonical injection $\operatorname{Hom}(A, \mathbf{U}) \to \operatorname{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mathbf{U})$. This follows from the commutativity of the natural diagram

$$\begin{array}{ccc} \Gamma_0(N) & \longrightarrow & H_1(X_0(N), \mathbf{Z}) \\ \downarrow & & \downarrow \\ (\mathbf{Z}/N\mathbf{Z})^\times & \longrightarrow & A \end{array} .$$

Since $J_0(N)$ is the set of complex points of the Jacobian variety $J_0(N)_{\mathbf{Q}}$ of $X_0(N)_{\mathbf{Q}}$, the Galois group $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, where $\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, acts on the group of torsion points of $J_0(N)$ and, in particular, on $\Sigma(N)$.

Let e be the exponent of the group $\Sigma(N)$ and let μ_e be the group of e-th roots of unity in $\mathbf{C}$. We can interprete ψ' as an injective homomorphism

$\Sigma(N) \to \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, \mu_e)$. Prop. 6 implies that this homomorphism is compatible with the actions of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (the action on $(\mathbf{Z}/N\mathbf{Z})^\times$ is trivial). Hence, each point of $\Sigma(N)$ is defined over $\mathbf{Q}(\mu_e)$, and $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q})$ acts on $\Sigma(N)$ via the cyclotomic character $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q}) \to (\mathbf{Z}/e\mathbf{Z})^\times$. Let x be an element of $\Sigma(N)$ and let e' be its order. The field of definition of x is the subfield of $\mathbf{Q}(\mu_e)$ fixed by the kernel of the composition of homomorphisms $\mathrm{Gal}(\mathbf{Q}(\mu_e)/\mathbf{Q}) \to (\mathbf{Z}/e\mathbf{Z})^\times \to (\mathbf{Z}/e'\mathbf{Z})^\times$, i.e., the cyclotomic field $\mathbf{Q}(\mu_{e'})$. In particular, $\mathbf{Q}(\mu_e)$ is the smallest extension of $\mathbf{Q}$ over which all points of $\Sigma(N)$ are defined. This completes the proof of thm. 2.

4.3 Points of $\Sigma(N)$ rational over $\mathbf{Q}$

Let x be a point of $\Sigma(N)$ and let e' be its order. We have shown in 4.2 that the field of definition of x is $\mathbf{Q}(\mu_{e'})$. In particular, x is rational over $\mathbf{Q}$ if and only if e' is equal to 1 or 2, i.e., if and only if we have $2x = 0$. This proves the first assertion of cor. 1 of thm. 2. To prove the last assertion, we shall, as in the statement of the corollary, denote by P the set of odd primes dividing N and by ϵ the number defined by

$$\epsilon = \begin{cases} -1 & \text{if } 4 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 8; \\ -1 & \text{if } 4|N, 8 \nmid N \text{ and there exists } p \in P,\ p \not\equiv 1 \bmod 4; \\ 1 & \text{if } 32|N; \\ 0 & \text{otherwise.} \end{cases}$$

By definition, the 2-rank of an abelian group A is the dimension of $A/2A$ over $\mathbf{Z}/2\mathbf{Z}$.

LEMMA 4 .— *Let A be a finite abelian group and let $a \in A$ be an element of order 2. The 2-rank of $A/\{0, a\}$ is equal to that of A if a belongs to $2A$, and is equal to that of A minus 1 otherwise.*

The lemma is obvious.

To complete the proof of cor. 1 of thm. 2, we have to show that the 2-rank of $\Sigma(N)$ is $\mathrm{Card}(P) + \epsilon$. If N is equal to 1, 2 or 4, the 2-rank of $\Sigma(N)$, $\mathrm{Card}(P)$ and ϵ are all equal to 0. We assume now that N is distinct from 1, 2 and 4, and distinguish between two cases:

a) *The case where* -1 *is a square* mod N.

The integer N is of the form N' or $2N'$, with $N' \neq 1$ and each prime factor of N' congruent to 1 mod 4. The quotient of the group

$$A = \prod_{p|N'} (\mathbf{Z}/\tfrac{p-1}{2}\mathbf{Z})$$

by the unique subgroup of order 2 which has a non-zero projection on each factor has the same 2-rank as $\Sigma(N)$ (2.3, cor. 1 of prop. 5). The 2-rank of A is $\mathrm{Card}(P)$. By lemma 4, the 2-rank of $\Sigma(N)$ is $\mathrm{Card}(P)$ or $\mathrm{Card}(P)-1$, depending on whether each prime factor of N' is congruent to 1 mod 8 or not, i.e., whether $\epsilon = 0$ or $\epsilon = -1$.

b) *The case where* -1 *is not a square* mod N.

Let r_2 be the exponent of 2 in the prime power decomposition of N. The quotient of the group

$$A = (\mathbf{Z}/2^{r_2-[r_2/2]}\mathbf{Z})^\times \times \prod_{p|N,p\neq 2} \mathbf{F}_p^\times$$

by the subgroup $\{-1,1\}$ (which is embedded diagonally in A) has the same 2-rank as $\Sigma(N)$ (2.3, cor. 2 of prop. 5, and isomorphism (21)).

Assume first that $r_2 \leq 2$. Then A is isomorphic to $\prod_{p|N,p\neq 2} \mathbf{F}_p^\times$, and its 2-rank is $\mathrm{Card}(P)$. By lemma 4, the 2-rank of $\Sigma(N)$ is $\mathrm{Card}(P)$ or $\mathrm{Card}(P)-1$, depending on whether the set P' of prime divisors of N congruent to 3 mod 4 is empty or not. If $r_2 = 0$ or $r_2 = 1$, P' is not empty because -1 is not a square mod N; we have $\epsilon = -1$ in this case by definition of ϵ. If $r_2 = 2$, we have $\epsilon = 0$ when $P' = \emptyset$ and $\epsilon = -1$ when $P' \neq \emptyset$, by definition of ϵ. This proves the announced formula for the 2-rank of $\Sigma(N)$ when $r_2 \leq 2$.

Assume now that $r_2 \geq 3$. Then $(\mathbf{Z}/2^{r_2-[r_2/2]}\mathbf{Z})^\times$ is the product of a cyclic group of order 2 onto which $\{-1,1\}$ maps surjectively and a cyclic group of order $2^{r_2'}$, where $r_2' = r_2 - [r_2/2] - 2$. The group $A/\{-1,1\}$ is therefore isomorphic to $\mathbf{Z}/2^{r_2'}\mathbf{Z} \times \prod_{p|N,p\neq 2} \mathbf{F}_p^\times$. Its 2-rank, equal to that of $\Sigma(N)$, is $\mathrm{Card}(P)$ or $\mathrm{Card}(P)+1$, depending on whether r_2' is equal to 0 (i.e., $r_2 = 3$ or $r_2 = 4$) or is at least 1 (i.e., $r_2 \geq 5$). In the first case, we have $\epsilon = 0$ and in the second case, $\epsilon = 1$, by definition of ϵ.

4.4 Cases where all points of $\Sigma(N)$ are rational over Q

By cor. 1 of thm. 2, all points of $\Sigma(N)$ are rational over Q if and only if the exponent of the group $\Sigma(N)$ is 1 or 2. The list of integers for which this is the case has been obtained in 3.3. In the 14 cases where the exponent of $\Sigma(N)$ is 2, the 2-rank of $\Sigma(N)$ can be computed by using cor. 1 of thm. 2 and the following table

N	20	21	24	32	48	64	72	96	100	144	147	192	288	576
Card(P)	1	2	1	0	1	0	1	1	1	1	2	1	1	1
ϵ	0	−1	0	1	0	1	0	1	0	0	−1	1	1	1

In all these cases, the 2-rank of $\Sigma(N)$ is equal to 1, except for $N = 96$, 192, 288 and 576 where it is equal to 2. Cor. 2 of thm. 2 follows.

5 Shimura subgroups and Atkin-Lehner involutions

To each divisor N_1 of N such that $\gcd(N_1, N/N_1) = 1$ is associated an Atkin-Lehner involution w_{N_1} of $X_0(N)$.

Analytic definition: The involution w_{N_1} is deduced, by passing to the quotients, from the transformation $\tau \mapsto g\tau$ of $\overline{\mathcal{H}}$, where $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is any matrix in $M_2(\mathbf{Z})$ such that $N_1|A$, $N_1|D$, $N|C$ and $AD - BC = N_1$. (Such a matrix g normalises $\Gamma_0(N)$.)

Modular description: The involution w_{N_1} stabilises $Y_0(N)$ and its restriction to $Y_0(N)$ has the following modular interpretation (with the conventions of 2.1, remark): if E is an elliptic curve over C and C a cyclic subgroup of E of order N, we have $w_{N_1}([E, C]) = [E/C_{N_1}, (E_{N_1} + C)/C_{N_1}]$, where C_{N_1} and E_{N_1} are the kernels of multiplication by N_1 in C and E respectively.

Let ${w_{N_1}}^*$ and $(w_{N_1})_*$ be the involutions of $J_0(N)$ deduced from w_{N_1} by Picard and Albanese functorialities. Since the holomorphic map w_{N_1} is of degree 1, we have $(w_{N_1})_* \circ {w_{N_1}}^* = \mathrm{Id}_{J_0(N)}$, and this implies $(w_{N_1})_* = {w_{N_1}}^*$ because ${w_{N_1}}^*$ is an involution.

By prop. 3 of 1.5, and 2.2, thm. 3 is a consequence of the following lemma:

LEMMA 5 .— *Let* $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *be as in the analytic definition of* w_{N_1} *given above. The automorphism* $\gamma \mapsto g\gamma g^{-1}$ *of* $\Gamma_0(N)$ *stabilises* $\Gamma_1(N)$. *The automorphism of* $(\mathbf{Z}/N\mathbf{Z})^\times$ $(\simeq \Gamma_0(N)/\Gamma_1(N))$ *which is deduced by passing to the quotients coincides with* $t \mapsto t^{-1}$ *modulo* N_1 *and with the identity modulo* N/N_1.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $\Gamma_0(N)$ and let $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be the matrix $g\gamma g^{-1}$. We have $d' = (-aBC + bAC - cBD + dAD)/N_1$. From the properties satisfied by g and from the fact that N divides c, we deduce that $-aBC, bAC, -cBD, dAD$ are respectively congruent to $aN_1, 0, 0, 0$ modulo N_1^2 and to $0, 0, 0, dN_1$ modulo N. Therefore, we have $d' \equiv a \equiv d^{-1} \bmod N_1$ and $d' \equiv d \bmod N/N_1$. This proves the lemma.

6 Shimura subgroups and degeneracy maps

6.1 Degeneracy maps

Let M be a divisor of N. For each divisor D of N/M, we have a holomorphic degeneracy map $v_D : X_0(N) \to X_0(M)$. It is the map deduced from the transformation $\tau \mapsto D\tau$ of $\overline{\mathcal{H}}$ by passing to the quotients. The map v_D induces a map from $Y_0(N)$ to $Y_0(M)$ which has the following modular interpretation (with the conventions of 2.1, remark): if E is an elliptic curve over $\mathbf{C}$ and C a cyclic subgroup of E of order N, we have

$$v_D([E, C]) = [E/C_D, C_{MD}/C_D],$$

where C_D and C_{MD} denote the unique subgroups of C of orders D and MD respectively. Let $v_D{}^* : J_0(M) \to J_0(N)$ and $(v_D)_* : J_0(N) \to J_0(M)$ denote the morphisms of abelian varieties deduced from v_D by Picard and Albanese functorialities.

6.2 Proof of thm. 4

By prop. 3 of 1.5, and 2.2, thm. 4 concerning the behaviour of the Shimura subgroups under the degeneracy maps $v_D{}^*$ is a consequence of the following lemma:

LEMMA 6 .— *Let g be the matrix $\begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix}$ and let $v : \Gamma_0(N) \to \Gamma_0(M)$ be the homomorphism $\gamma \mapsto g\gamma g^{-1}$. We have $v(\Gamma_1(N)) \subseteq \Gamma_1(M)$ and v induces, by passing to the quotients, the canonical surjection $(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/M\mathbf{Z})^\times$.*

Lemma 6 follows from the identity

$$\begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & bD \\ c/D & d \end{pmatrix}.$$

6.3 A compatibility property of transfer homomorphisms

In this section, G denotes a group and H denotes a subgroup of G. We denote by $\iota_{G,H} : H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ the homomorphism deduced from the canonical injection $H \to G$. If the index $[G : H]$ is finite, $V_{H,G} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ denotes the transfer homomorphism.

LEMMA 7 .— *Let G' be a subgroup of G such that $G = HG'$ (i.e., such that G' maps surjectively to $H\backslash G$) and let H' be a subgroup of $H \cap G'$ of finite index in G'. Then $[G : H]$ is finite, the quotient $r = [G' : H']/[G : H]$ is equal to $[H \cap G' : H']$ and the diagram*

$$\begin{array}{ccc} G'^{\mathrm{ab}} & \xrightarrow{V_{H',G'}} & H'^{\mathrm{ab}} \\ {\scriptstyle \iota_{G,G'}}\downarrow & & \downarrow{\scriptstyle \iota_{H,H'}} \\ G^{\mathrm{ab}} & \xrightarrow{V^r_{H,G}} & H^{\mathrm{ab}}, \end{array}$$

where $V^r_{H,G}$ denotes the homomorphism $x \mapsto (V_{H,G}(x))^r$, is commutative.

In the proof, let us write the groups additively and consider the diagram

$$\begin{array}{ccccc} G'^{\mathrm{ab}} & \xrightarrow{V_{H\cap G',G'}} & (H \cap G')^{\mathrm{ab}} & \xrightarrow{V_{H',H\cap G'}} & H'^{\mathrm{ab}} \\ {\scriptstyle \iota_{G,G'}}\downarrow & & {\scriptstyle \iota_{H,H\cap G'}}\downarrow & & {\scriptstyle \iota_{H,H'}}\downarrow \\ G^{\mathrm{ab}} & \xrightarrow{V_{H,G}} & H^{\mathrm{ab}} & \xrightarrow{r.1_{H^{\mathrm{ab}}}} & H^{\mathrm{ab}}. \end{array} \qquad (23)$$

The canonical map $H \cap G'\backslash G' \to H\backslash G$ is bijective by hypothesis, hence H is of finite index in G, we have $[G' : H'] = [G : H][H \cap G' : H']$ and a system

of representatives in G' of $H \cap G' \backslash G'$ is also a system of representatives in G of $H \backslash G$. The first square of diagram (23) is therefore commutative, by definition of the transfer homomorphisms (1.5). This definition also implies that $\iota_{H\cap G',H'} \circ V_{H',H\cap G'}$ coincides with multiplication by $r = [H \cap G' : H']$ in $(H \cap G')^{\mathrm{ab}}$, and the commutativity of the second square of diagram (23) follows. Since the transfer homomorphisms satisfy the transitivity property $V_{H',H\cap G'} \circ V_{H\cap G',G'} = V_{H',G'}$ ([2], thm. 14.2.1), the commutativity of diagram (23) establishes the lemma.

6.4 The transfer homomorphism $\Gamma_0(M)^{\mathrm{ab}} \to \Gamma_0(N)^{\mathrm{ab}}$

Let M be a divisor of N, $\iota_{M,N} : \Gamma_0(N)^{\mathrm{ab}} \to \Gamma_0(M)^{\mathrm{ab}}$ the homomorphism deduced from the injection $\Gamma_0(N) \to \Gamma_0(M)$, $V_{N,M} : \Gamma_0(M)^{\mathrm{ab}} \to \Gamma_0(N)^{\mathrm{ab}}$ the transfer homomorphism, and $\pi_N : \Gamma_0(N)^{\mathrm{ab}} \to (\mathbf{Z}/N\mathbf{Z})^\times$ the surjection deduced from our identification of $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbf{Z}/N\mathbf{Z})^\times$.

In the next proposition, we use the following notation: for an integer n, $n^\star$ denotes n when n is odd and $n/2$ when n is even. We also write $N = N_1 N_2$, with N_2 the largest divisor of N prime to M.

PROPOSITION 7 .— *Let* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be an element of* $\Gamma_0(M)$ *and* $\overline{\gamma}$ *its image in* $\Gamma_0(M)^{\mathrm{ab}}$. *The element* $\pi_N(V_{N,M}(\overline{\gamma}))$ *of* $(\mathbf{Z}/N\mathbf{Z})^\times$ *is congruent to* $d^{[\Gamma_0(M):\Gamma_0(N)]}$ *modulo* $N_1^\star$ *and to* 1 *modulo* $N_2^\star$.

Let p be a prime divisor of N. Let us write $M = p^m M'$, $N = p^n N'$, with M' and N' prime to p. The map $\Gamma_0(p^n)\backslash SL_2(\mathbf{Z}) \to \mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$ which sends a coset $\Gamma_0(p^n)\begin{pmatrix} u & v \\ w & t \end{pmatrix}$ to the point of $\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$ with homogeneous coordinates (w, t) is bijective. Therefore the canonical map $\Gamma_0(M) \to \Gamma_0(p^n)\backslash\Gamma_0(p^m)$ is surjective. By applying lemma 7, we get a commutative diagram

$$\begin{array}{ccccc} \Gamma_0(M)^{\mathrm{ab}} & \xrightarrow{V_{N,M}} & \Gamma_0(N)^{\mathrm{ab}} & \xrightarrow{\pi_N} & (\mathbf{Z}/N\mathbf{Z})^\times \\ \downarrow{\scriptstyle \iota_{p^m,M}} & & \downarrow{\scriptstyle \iota_{p^n,N}} & & \downarrow \\ \Gamma_0(p^m)^{\mathrm{ab}} & \xrightarrow{V^r_{p^n,p^m}} & \Gamma_0(p^n)^{\mathrm{ab}} & \xrightarrow{\pi_{p^n}} & (\mathbf{Z}/p^n\mathbf{Z})^\times, \end{array} \tag{24}$$

where r is equal to $[\Gamma_0(M) : \Gamma_0(N)]/[\Gamma_0(p^m) : \Gamma_0(p^n)]$ and the last vertical map is the canonical surjection. This shows that, in order to prove the "p-primary part" of the congruences of prop. 7, it is sufficient to prove

prop. 7 when N is a power of p. From now on, we make this assumption. We consider two cases:

a) *The case* $m \geq 1$

In this case, we have $N_1 = N = p^n$, $N_2 = 1$, $M = p^m$ and the matrices $s_l = \begin{pmatrix} 1 & 0 \\ lM & 1 \end{pmatrix}$, with $1 \leq l \leq N/M$, form a system of representatives of $\Gamma_0(N)\backslash\Gamma_0(M)$. For each integer l, $1 \leq l \leq N/M$, there exists a unique integer k such that $1 \leq k \leq N/M$ and $alM + c \equiv kM(blM + d) \bmod N$; the identity

$$\begin{pmatrix} 1 & 0 \\ lM & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - bkM & b \\ alM + c - kM(blM + d) & blM + d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ kM & 1 \end{pmatrix}$$

shows that we have $s_l\gamma = a_{l,\gamma}s_k$ with $a_{l,\gamma}$ in $\Gamma_0(N)$, and that $\pi_N(\overline{a_{l,\gamma}})$ is the class of $blM + d \bmod N$. By definition of the transfer homomorphism (see 1.5), $\pi_N(V_{N,M}(\overline{\gamma}))$ is equal to $\prod_{1\leq l\leq N/M} \pi_N(\overline{a_{l,\gamma}})$, i.e., to the class mod N of $\prod_{1\leq l\leq N/M} (blM + d)$. From this, we deduce

$$\pi_N(V_{N,M}(\overline{\gamma})) = d^{N/M}(\prod_{h\in H} h)^{M'/M}, \tag{25}$$

where M' is given by $M' = \gcd(bM, N)$ and H denotes the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ consisting of the elements congruent to 1 mod M'.

LEMMA 8 .— *Let A be a finite abelian group. The product of the elements of A is equal to the unit element, except in the case where A has a unique element ϵ of order 2; in that case, the product is equal to ϵ.*

The lemma is immediately proved by writing A as a product of cyclic groups.

We now apply the lemma to the subgroup H of $(\mathbf{Z}/N\mathbf{Z})^\times$. The only cases where H has a unique element of order 2 are those where we have $p = 2$, and either $(M', N) = (2, 4)$ or $4 \leq M' < N$. In these cases, $\prod_{h\in H} h$ is the class of $1 + (N/2) \bmod N$; in all the other cases, $\prod_{h\in H} h$ is the class of 1 mod N. From (25), we therefore deduce the congruence

$$\pi_N(V_{N,M}(\overline{\gamma})) \equiv d^{N/M} \bmod N^*. \tag{26}$$

Since we have $N/M = p^{n-m} = [\Gamma_0(M) : \Gamma_0(N)]$, prop. 7 follows.

b) *The case* $m = 0$

In this case, we have $N_1 = M = 1$, $N_2 = N = p^n$. Since prop. 7 is obvious when $N = 1$, we may assume $n \geq 1$. The group $\Gamma_0(M)$ is equal to $SL_2(\mathbf{Z})$. It is isomorphic to the group given by the presentation $\langle s, u; s^4, u^6, s^2u^{-3}\rangle$ ([6], p.52): an isomorphism between this latter group and $SL_2(\mathbf{Z})$ is obtained by sending s to $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and u to TS, where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (*loc. cit.*). The group $SL_2(\mathbf{Z})^{\mathrm{ab}}$ is hence isomorphic to the group defined by the presentation $\langle s, u; s^4, u^6, s^2u^{-3}, sus^{-1}u^{-1}\rangle$, i.e., (by taking $v = u^2$) to the group defined by the presentation $\langle s, v; s^4, v^3, svs^{-1}v^{-1}\rangle$. It is a cyclic group of order 12. Let $\overline{S}$ and $\overline{T}$ denote the canonical images of S and T in $SL_2(\mathbf{Z})^{\mathrm{ab}}$. The subgroup of order 4 of $SL_2(\mathbf{Z})^{\mathrm{ab}}$ is generated by $\overline{S}$ and the subgroup of order 3 by $(\overline{T}\,\overline{S})^2 = \overline{S}^2(\overline{T}\,\overline{S})^{-1} = \overline{S}\,\overline{T}^{-1}$. This implies that $\overline{T}$ generates $SL_2(\mathbf{Z})^{\mathrm{ab}}$. In order to prove prop. 7, it suffices to treat the case where the matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

The matrices $s_l = \begin{pmatrix} 1 & 0 \\ lp & 1 \end{pmatrix}$, for $1 \leq l \leq N/p$, and $s'_j = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$, for $1 \leq j \leq N$, form a system of representatives of $\Gamma_0(N)\backslash SL_2(\mathbf{Z})$. For each integer l, $1 \leq l \leq N/p$, there exists a unique integer k such that $1 \leq k \leq N/p$ and $l \equiv k(1 + lp) \bmod N/p$, and the identity

$$\begin{pmatrix} 1 & 0 \\ lp & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 - kp & 1 \\ lp - kp(1 + lp) & 1 + lp \end{pmatrix}\begin{pmatrix} 1 & 0 \\ kp & 1 \end{pmatrix}$$

shows that $s_l T = a_l s_k$, with a_l in $\Gamma_0(N)$ and $\pi_N(\overline{a_l}) = 1 + lp \bmod N$. Furthermore, we have

$$s'_j T = s'_{j+1} \qquad \text{for } 1 \leq j < N$$

$$s'_N T = \begin{pmatrix} 1 & 0 \\ -N & 1 \end{pmatrix} s'_1.$$

By definition of the transfer homomorphism, $\pi_N(V_{N,1}(\overline{T}))$ is then the class mod N of $\prod_{1 \leq l \leq N/p}(1 + lp)$. By lemma 8, this class is equal to 1 mod N, except in the case $N = 4$, where it is equal to 3 mod N. Prop. 7 follows.

6.5 Proof of thm. 5

Let M be a divisor of N, and D a divisor of N/M. As in 6.4, we write $N = N_1 N_2$, with N_2 the largest divisor of N prime to M. The index $[\Gamma_0(M) : \Gamma_0(N)]$ is equal to $\frac{N}{M} \prod_{p|N_2} (1+\frac{1}{p})$, hence is a multiple of N_1/M. Since N_1 and M have the same prime divisors, this implies that, if d is an integer prime to M, the class $d^{[\Gamma_0(M):\Gamma_0(N)]}$ mod N_1 depends only on d mod M. We can therefore define a homomorphism $\delta' : (\mathbf{Z}/M\mathbf{Z})^\times \to (\mathbf{Z}/N\mathbf{Z})^\times$ by the following relations:

$$\begin{cases} \delta'(d + M\mathbf{Z}) \equiv d^{[\Gamma_0(M):\Gamma_0(N)]} & \mod N_1 \\ \delta'(d + M\mathbf{Z}) \equiv 1 & \mod N_2. \end{cases}$$

By prop. 4 of 1.5, and 2.2, thm. 5 concerning the behaviour of the Shimura subgroup of $J_0(N)$ under the morphism $(v_D)_* : J_0(N) \to J_0(M)$ (which was defined in 6.1) is equivalent to the following statement: the diagram

$$\begin{array}{ccccc} \Gamma_0(M)^{\mathrm{ab}} & \longrightarrow & \Gamma_0(M)/\Gamma_1(M) \simeq & (\mathbf{Z}/M\mathbf{Z})^\times \\ V \downarrow & & & \downarrow \delta' \\ \Gamma_0(N)^{\mathrm{ab}} & \longrightarrow & \Gamma_0(N)/\Gamma_1(N) \simeq & (\mathbf{Z}/N\mathbf{Z})^\times. \end{array} \qquad (27)$$

where V is the transfer homomorphism and the horizontal arrows represent the canonical surjections, is commutative modulo J, where J is the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ defined in 2.3.

Prop. 7 tells us that (27) is commutative when $4 \nmid N$, and that (27) is commutative modulo the subgroup of order 2 of $(\mathbf{Z}/N\mathbf{Z})^\times$ generated by the class d of $1 + (N/2)$ mod N, when $4|N$. In the latter case, we have $(d-1)^2 = 0$ in $\mathbf{Z}/N\mathbf{Z}$, hence d belongs to J. This completes the proof of thm. 5.

7 Action of the Hecke algebra on the Shimura subgroup

Let p be a prime number. The two degeneracy maps

$$\begin{array}{ccccc} & & X_0(Np) & & \\ & {\scriptstyle v_p}\swarrow & & \searrow{\scriptstyle v_1} & \\ X_0(N) & & & & X_0(N) \end{array}$$

define a correspondence T_p between $X_0(N)$ and itself: we have $T_p = v_1 \circ v_p^{-1}$, where the symbol v_p^{-1} denotes the inverse correspondence of v_p and $\circ$ denotes the composition of correspondences.

If $[\tau]$ denotes the image in $X_0(N)$ of a point $\tau \in \overline{\mathcal{H}}$, then T_p is given by

$$T_p([\tau]) = \begin{cases} [p\tau] + \sum\limits_{0 \le i \le p-1} \left[\frac{\tau+i}{p}\right] & \text{if } p \nmid N \\ \\ \sum\limits_{0 \le i \le p-1} \left[\frac{\tau+i}{p}\right] & \text{if } p \mid N. \end{cases}$$

The restriction of T_p to $Y_0(N)$ has the following modular interpretation: if E is an elliptic curve defined over $\mathbf{C}$ and C a cyclic subgroup of order N of E, then

$$T_p([E, C]) = \sum_{C'} [E/C', (C + C')/C'],$$

where the sum is indexed by the subgroups C' of E of order p, with the restriction that $C \cap C' = \{0\}$ if p divides N.

We can define endomorphisms ${T_p}^*$ and $(T_p)_*$ of $J_0(N)$ by

$$\begin{aligned} {T_p}^* &= (v_p)_* \circ {v_1}^* \\ (T_p)_* &= (v_1)_* \circ {v_p}^*. \end{aligned} \tag{28}$$

(When we think of a correspondence as an object generalising a map, ${T_p}^*$ and $(T_p)_*$ can be thought of as associated to T_p via Picard and Albanese functorialities respectively; however, the definition of each of them involves both functorialities, as is seen in the formulae.)

Theorems 4 and 5 imply that both the endomorphisms ${T_p}^*$ and $(T_p)_*$ stabilise the Shimura subgroup $\Sigma(N)$ of $J_0(N)$, and that they coincide on $\Sigma(N)$ with multiplication by $[\Gamma_0(N) : \Gamma_0(Np)]$, i.e., by $p+1$ if p does not divide N, and by p if p divides N. This proves thm. 6.

It is possible to define, for each integer $n \ge 1$, a Hecke correspondence T_n on $X_0(N)$ and, hence, endomorphisms ${T_n}^*$ and $(T_n)_*$ of $J_0(N)$. The endomorphisms ${T_n}^*$ satisfy recurrence relations which can be summarised by the formal identity between Dirichlet series

$$\sum {T_n}^* n^{-s} = \prod_{p \mid N} (1 - {T_p}^* p^{-s})^{-1} \prod_{p \nmid N} (1 - {T_p}^* p^{-s} + p^{1-2s})^{-1},$$

and we have an analogous identity for $(T_n)_*$. Therefore, remark 2 in the introduction follows from the identity

$$\sum_{n=1}^{\infty} a_N(n) n^{-s} = \prod_{p|N} (1 - p^{1-s})^{-1} \prod_{p \nmid N} (1 - p^{-s})(1 - p^{1-s})^{-1},$$

where $a_N(n)$ denotes the sum of the divisors d of n satisfying the condition $\gcd(N, \frac{n}{d}) = 1$.

References

[1] A. GROTHENDIECK, *Éléments de Géométrie algébrique*, chapitre II, Publications mathématiques de l'I.H.E.S., Vol. 8, 1961.

[2] M. HALL Jr., *The theory of groups*, The Macmillan Cy., New York, 1959.

[3] B. MAZUR, *Modular curves and the Eisenstein ideal*, Publications mathématiques de l'I.H.E.S., Vol. 47, 1978, pp. 33–186.

[4] M. RAYNAUD, *Familles de fibrés vectoriels sur une surface de Riemann* [d'après C. S. Seshadri, M. S. Narasimhan et D. Mumford], Séminaire Bourbaki 1966/1967, exposé 316.

[5] K. A. RIBET, *On the component groups and the Shimura subgroup of $J_0(N)$*, séminaire de théorie des nombres de Bordeaux, 1987–1988, exposé 6.

[6] J.-P. SERRE, *Arbres, amalgames, SL_2*. Astérisque, Vol. 46, 1977.

[7] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, copublished by Iwonami Shoten and Princeton University Press, 1971.

LING San
Mathematics Department
University of California
Berkeley CA 94720
U.S.A.

OESTERLÉ Joseph
Département de mathématiques
Université de Paris VI
4, place Jussieu
75005 PARIS
FRANCE