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.

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

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

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

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

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 $g : (\mathbf{Z}/N\mathbf{Z})^\times \rightarrow \mathbf{U}$ 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* $\underset{p|N}{\mathrm{lcm}}((p-1)p^{r'_p})$*;*

(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*

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

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*

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

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