Modular curves

Benjamin Schraen

1 First examples

1.1 Elliptic functions

A *lattice* of the field of complex number $\mathbb{C}$ is an additive subgroup of $\mathbb{C}$ generated by an $\mathbb{R}$-basis of $\mathbb{C}$. Equivalently it is a discrete subgroup Λ such that $\mathbb{C}/\Lambda$ is compact. For example, $\mathbb{Z}+\mathbb{Z}i$, $\mathbb{Z}+\mathbb{Z}e^{2\pi i/3}$ or $\mathbb{Z}\sqrt{5}+\mathbb{Z}(1+i\sqrt{7})/2$ are examples of lattices. However the finite free $\mathbb{Z}$-module $\mathbb{Z}+\mathbb{Z}\sqrt{5}$ is not a lattice : it does not contain any basis of $\mathbb{C}$ as a $\mathbb{R}$-vector space nor is discrete.

A *complex torus* is a complex analytic group of the form $\mathcal{E}_\Lambda := \mathbb{C}/\Lambda$ where Λ is a lattice of $\mathbb{C}$.

Let $\Lambda \subset \mathbb{C}$ be a lattice in $\mathbb{C}$. An *elliptic function* for Λ is a meromorphic function on the Riemann surface $\mathcal{E}_\Lambda$. An elliptic function can also be viewed as a meromorphic function f defined over $\mathbb{C}$ such that

$$\forall \lambda \in \Lambda, \quad f(z+\lambda) = f(z).$$

Recall that for $P \in \mathbb{C}$ and f be a meromorphic function, we note the $\mathrm{ord}_P(f)$ the order of vanishing of f at P. We have $\mathrm{ord}_P f > 0$ if and only if P is a zero of f and $\mathrm{ord}_P f < 0$ if and only if P is a pole of f.

A *fundamental domain* of the lattice Λ is a subset of $\mathbb{C}$ of the form $M(P;\omega_1,\omega_2) = \{P + a\omega_1 + b\omega_2 \mid (a,b) \in [0,1[^2\}$ where P a point of $\mathbb{C}$ and (ω_1,ω_2) is a basis of the lattice Λ.

If we apply the Residues Formula to the functions $z \mapsto f'(z)/f(z)$ and $z \mapsto zf'(z)/f(z)$ on the boundary of a fundamental domain $M(P;\omega_1,\omega_2)$ whose boundary does not contain any zero or pole of f and such that moreover $0 \notin \overline{M(P;\omega_1,\omega_2)}$, we obtain

$$2\pi i \sum_{Q \in M} \mathrm{ord}_Q(f) = \left(\int_P^{P+\omega_1} \frac{f'(z)}{f(z)}\,\mathrm{d}z + \int_{P+\omega_1}^{P+\omega_1+\omega_2} \frac{f'(z)}{f(z)}\,\mathrm{d}z \right.$$
$$\left. + \int_{P+\omega_1+\omega_2}^{P+\omega_2} \frac{f'(z)}{f(z)}\,\mathrm{d}z + \int_{P+\omega_2}^{P} \frac{f'(z)}{f(z)}\,\mathrm{d}z \right) = 0.$$

$$2\pi i \sum_{P\in\mathcal{E}_\Lambda} P \operatorname{ord}_P f = \int_0^1 \omega_1 f(P+t\omega_1)\,\mathrm{d}t + \int_0^1 \omega_2 f(P+\omega_1+t\omega_2)\,\mathrm{d}t$$
$$- \int_0^1 \omega_1 f(P+t\omega_1+\omega_2)\,\mathrm{d}t - \int_0^1 \omega_2 f(P+t\omega_2)\,\mathrm{d}t \in \Lambda.$$

This implies that for each elliptic function f of lattice Λ, we have the equalities

$$\begin{cases} \sum_{P\in\mathcal{E}_\Lambda} \operatorname{ord}_P f = 0 \\ \sum_{P\in\mathcal{E}_\Lambda} P \operatorname{ord}_P f = 0_{\mathcal{E}_\Lambda}. \end{cases} \tag{1}$$

Theses formulas imply in particular that a non constant elliptic function must have at least one pole and if this pole is unique in $\mathcal{E}_\Lambda$, this pole must be of order at least 2.

We now give our first concrete example of elliptic function.

Example 1.1. The *Weierstrass function* $\mathfrak{p}_\Lambda$ is the meromorphic function defined by the following series, converging normally on every compact subset of $\mathbb{C}\smallsetminus\Lambda$:

$$\mathfrak{p}(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda\smallsetminus\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right).$$

If f is an elliptic function, so are all the derivative in f and the rational functions in these derivative. Consequently we can produce a large amount of elliptic functions from $\mathfrak{p}_\Lambda$.

In order to determine the relations existing between all these elliptic functions, we can compare their developments around 0. For $\lambda\in\Lambda\smallsetminus\{0\}$ and $|z|<|\lambda|$, we have

$$\frac{1}{z-\lambda} = -\frac{1}{\lambda}\sum_{n\geqslant 0}\left(\frac{z}{\lambda}\right)^n$$

with normal convergence on each compact. After derivation we obtain

$$\frac{1}{(z-\lambda)^2} = \sum_{n\geqslant 1} n\frac{z^{n-1}}{\lambda^{n+1}}.$$

Let $n(\Lambda) \coloneqq \min\{|\lambda| \mid \lambda\in\Lambda\smallsetminus\{0\}\}$. For $0<|z|\leqslant r<n(\Lambda)$, we have

$$\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\sum_{n\geqslant 1}(n+1)\frac{|z|^n}{|\lambda|^{n+2}} \leqslant \sum_{n\geqslant 1}(n+1)\left(\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\frac{1}{\lambda^{n+2}}\right)z^n.$$

We introduce the notation $G_k(\Lambda) \coloneqq \sum_{\lambda\in\Lambda\smallsetminus\{0\}}\frac{1}{\lambda^n}$ for $k\geqslant 3$. If k is odd, it is clear that $G_k(\Lambda)=0$ so that

$$\mathfrak{p}(z) = \frac{1}{z^2} + \sum_{n\geqslant 1}(2n+1)G_{2n+2}(\Lambda)z^{2n}$$
$$\mathfrak{p}'(z) = -\frac{2}{z^3} + \sum_{n\geqslant 1}2n(2n+1)G_{2n+2}(\Lambda)z^{2n-1}.$$

Using these developments we see that

$$(\mathfrak{p}')^2 - 4\mathfrak{p}^3 + 60G_4(\Lambda)\mathfrak{p} + 140G_6(\Lambda)$$

is an elliptic function without pole and vanishing at 0, hence identically 0. Finally we see that the elliptic function $\mathfrak{p}$ satisfies the differential equation

$$(\mathfrak{p}')^2 = 4\mathfrak{p}^3 - g_4(\Lambda)\mathfrak{p} - g_6(\Lambda)$$

where $g_4 = 60G_4$ and $g_6 = 140G_6$.

For an elliptic function f, we define

$$\deg(f) \coloneqq \sum_{\substack{P \in \mathcal{E}_\Lambda \\ \operatorname{ord}_P f > 0}} \operatorname{ord}_P f = - \sum_{\substack{P \in \mathcal{E}_\Lambda \\ \operatorname{ord}_P f < 0}} \operatorname{ord}_P f.$$

Looking at poles, we deduce that $\deg(f - a) = \deg f$ for all $a \in C$ so that $\deg(f)$ is the number of roots counted with multiplicities of the equation $\mathfrak{p}(z) = a$ in $\mathcal{E}_\Lambda$. As a particular case, if f is non constant, for all $a \in \mathbb{C}$, the equation $f(z) = a$ has a solution. More geometrically, if f is non constant, $\deg f$ is the degree of the finite morphism of Riemann surfaces $\mathcal{E}_\Lambda \to \mathbb{P}^1(\mathbb{C})$ defined by f.

Lemma 1.2. *We have* $\deg(\mathfrak{p}) = 2$ *and for* $a \in \mathbb{C}$, $\mathfrak{p} - a$ *has exactly one zero of order* 2 *if and only if* $a = \mathfrak{p}(\omega)$ *with* $2\omega \in \Lambda$ *and* $\omega \notin \Lambda$. *Otherwise* $\mathfrak{p} - a$ *has exactly two simple zeros* P_1 *and* P_2 *in* $\mathcal{E}_\Lambda$ *such that* $P_1 = -P_2$ *in* $\mathcal{E}_\Lambda$. *We have* $\deg(\mathfrak{p}') = 3$ *and* $\mathfrak{p}'$ *has exactly three simple zeros which are the* $\omega \in \mathcal{E}_\Lambda$ *such that* $\mathfrak{p} - \mathfrak{p}(\omega)$ *has a double zero.*

Proof. For all $a \in \mathbb{C}$, the function $\mathfrak{p} - a$ has a unique pole of order -2 in $\mathcal{E}_\Lambda$ so that $\deg(\mathfrak{p} - a) = 2$. The same argument shows that $\deg \mathfrak{p}' = 3$. Consequently $\mathfrak{p} - a$ has either 1 zero of order 2 or two simple zeros in $\mathcal{E}_\Lambda$. If ω is a zero of order $n \geqslant 1$ of $\mathfrak{p}'$, then ω is a zero of order $n + 1$ of $\mathfrak{p} - \mathfrak{p}(\omega)$. Consequently $n = 1$ and $\mathfrak{p}'$ has exactly 3 zeros. Moreover these zeros are exactly the values ω such that $\mathfrak{p} - \mathfrak{p}(\omega)$ has a zero of order 2. The function $\mathfrak{p}'$ being odd, an element $\omega \in \mathcal{E}_\Lambda \smallsetminus \{0\}$ such that $\omega = -\omega$ in $\mathcal{E}_\Lambda$ satisfy $\mathfrak{p}'(\omega) = 0$. There are exactly three elements in $\mathcal{E}_\Lambda$ having this property so that we can conclude. □

Theorem 1.3. *The field of elliptic functions of lattice* Λ *is the field* $\mathbb{C}(\mathfrak{p}, \mathfrak{p}')$ *of rational functions in* $\mathfrak{p}$ *and* $\mathfrak{p}'$. *The subfield* $\mathbb{C}(\mathfrak{p})$ *is exactly the field of even elliptic functions.*

Proof. As $\mathfrak{p}'$ is an odd non zero elliptic function, each elliptic function can be uniquely written as $f_1 + \mathfrak{p}' f_2$ with f_1 and f_2 even elliptic functions. It is therefore sufficient to prove the second assertion. Let f be some even elliptic function. Let $\omega \in \mathcal{E}_\Lambda$. As f is even, if $\omega \in \frac{1}{2}\Lambda$, then $\operatorname{ord}_\omega(f)$ is even. This implies that, multiplying f by some polynomial in $\mathfrak{p}$, we can kill the poles of f, excepted poles at points of Λ. We are reduced to prove that an even elliptic function having poles only at points of Λ is a polynomial in $\mathfrak{p}$. If f is such a function, its Laurent development at 0 contains only even terms,

consequently we can find some polynomial $P \in \mathbb{C}[X]$ such that $f - P(\mathfrak{p})$ is vanishing at 0 and consequently has no pole on $\mathbb{C}$. This implies that $f - P(\mathfrak{p})$ is constant and vanishing at 0 hence is zero. □

Let Λ and Λ' be two lattices in $\mathbb{C}$ and $\alpha \in \mathbb{C}$ be a complex number such that $\alpha\Lambda \subset \Lambda'$. Then the map $\mathcal{E}_\Lambda \to \mathcal{E}_{\Lambda'}$ defined by $z \mapsto \alpha z$ is an endomorphism of complex analytic Lie groups. The following result says we obtain all possible endomorphism by this process.

Proposition 1.4. *Let $f : \mathcal{E}_\Lambda \to \mathcal{E}_{\Lambda'}$ be an endomorphism of complex elliptic curves. Then there exists a unique $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subset \Lambda'$ and $f(z) = \alpha z$.*

Proof. The quotient map $\pi_\Lambda : \mathbb{C} \to \mathbb{C}/\Lambda$ is a topological covering. The topological space $\mathbb{C}$ being simply connected, there exists a unique continuous map $\tilde{f}$ from $\mathbb{C}$ to $\mathbb{C}$ such that $\pi_{\Lambda'} \circ \tilde{f} = f \circ \pi_\Lambda$ and $f(0) = 0$. As f is a Lie group homomorphism, as are π_Λ and $\pi_{\Lambda'}$, the map $\tilde{f}$ is a Lie group homomorphism. Such a map is necessarily of the form $z \mapsto \alpha z$ for some α. Finally $\tilde{f}$ sends $\operatorname{Ker}\pi_\Lambda$ inside $\operatorname{Ker}\pi_{\Lambda'}$ which gives us $\tilde{f}(\Lambda) \subset \Lambda'$. □

Corollary 1.5. *Two elliptic curves $\mathcal{E}_\Lambda$ and $\mathcal{E}_{\Lambda'}$ are isomorphic if and only if the lattices Λ and Λ' are homothetic.*

1.2 First examples of modular functions

Let $\mathbb{H}$ be the *Poincaré upper half plane* defined by

$$\mathbb{H} \coloneqq \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}.$$

If $\tau \in \mathbb{H}$ we set $\Lambda_\tau \coloneqq \mathbb{Z}\tau + \mathbb{Z}$. It is a lattice of $\mathbb{C}$. We note E_τ the elliptic curve $\mathcal{E}_{\Lambda_\tau}$.

Proposition 1.6. *Every lattice of $\mathbb{C}$ is homothetic to a lattice of the form Λ_τ for some $\tau \in \mathbb{H}$. Moreover two lattices Λ_τ and $\Lambda_{\tau'}$ are homothetic if and only if there exists $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that*

$$\tau' = \frac{a\tau + b}{c\tau + d}.$$

In this case we have $\Lambda_{\frac{a\tau+b}{c\tau+d}} = (c\tau + d)^{-1}\Lambda_\tau$.

Proof. Let (ω_1, ω_2) be some basis of a lattice Λ. Up to exchanging ω_1 and ω_2 we can assume that $\operatorname{Im}(\omega_1/\omega_2) > 0$ and we have $\Lambda = \omega_2\Lambda_{\omega_1/\omega_2}$. This proves the first assertion.

For the second assertion, the lattices Λ_τ and $\Lambda_{\tau'}$ are homothetic if and only if there exists $\alpha \in \mathbb{C}^\times$ such that $\Lambda_{\tau'} = \alpha\Lambda_\tau$ this is equivalent to the existence of $\alpha \in \mathbb{C}^\times$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$\begin{cases} \tau' &= \alpha(a\tau + b) \\ 1 &= \alpha(c\tau + d). \end{cases}$$

This system is equivalent to the existence of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $\tau' = \frac{a\tau+b}{c\tau+d}$. Finally, if $\tau \in \mathbb{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, we have $ad-bc = \pm 1$ and $\frac{a\tau+b}{c\tau+d} \in \mathbb{H}$ if and only if $ad - bc = 1$. □

If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we set

$$\forall \tau \in \mathbb{H},\ \gamma \cdot \tau \coloneqq \frac{a\tau + b}{c\tau + d}.$$

The law $(\gamma, \tau) \mapsto \gamma \cdot \tau$ is a left group action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

Corollary 1.7. *The map $\tau \mapsto E_\tau$ induces a bijection between the orbit set $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and the set of isomorphism classes of complex elliptic curves.*

The elliptic curves E_τ and $E_{\gamma\cdot\tau}$ are isomorphic but the Weierstrass equation associated to the lattices Λ_τ and $\Lambda_{\gamma\tau}$ might be different. Namely, for $\alpha \in \mathbb{C}^\times$, Λ a lattice of $\mathbb{C}$ and $k \geqslant 4$, we have the law

$$G_k(\alpha\Lambda) = \alpha^{-k} G_k(\Lambda).$$

Consequently if we define a function G_k on $\mathbb{H}$ by the formula $G_k(\tau) \coloneqq G_k(\Lambda_\tau)$, we obtain a holomorphic function G_k defined over $\mathbb{H}$ and satisfiying the transformation law

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \forall \tau \in \mathbb{H},\ G_k\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k G_k(\tau).$$

Such a function is called a *weakly modular form of weight k*.

As a consequence, the function G_k is holomorphic and $\mathbb{Z}$-periodic. Let $D \coloneqq \{q \in \mathbb{C} \mid |q| < 1\}$ and $D^* \coloneqq D \smallsetminus \{0\}$. The holomorphic map $\mathbb{H} \to D^*$ defined by $\tau \mapsto e^{2\pi i\tau}$ is actually a covering map. This implies that, for all $k \geqslant 4$, there exists a holomorphic function $\tilde{G_k}$ on D^* such that $G_k(\tau) = \tilde{G_k}(e^{2\pi i\tau})$.

Theorem 1.8. *For $k \geqslant 2$, we have*

$$\tilde{G_{2k}}(q) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n \geqslant 1} \left(\sigma_{2k-1}(n)\right) q^n$$

where $\sigma_m(n) \coloneqq \sum_{\substack{d \geqslant 1 \\ d|n}} d^{m-1}$.

Exercice 1.1. Prove that, for $z \in \mathbb{C}$, $\pi \cot(\pi z) = \sum_{n\in\mathbb{Z}} (z-n)^{-1}$. Deduce Theorem 1.8.

The function $\tilde{G_{2k}}$ is actually an holomorphic function on D, we say that it is a *weakly modular form of weight $2k$* which is holomorphic at infinity. We will call later such a function a *modular form of weight $2k$*.

The values of the function ζ at positive even integers are given by the formula

$$\forall k \geqslant 1,\ \zeta(2k) = -\frac{1}{2}\frac{(2\pi i)^{2k} B_{2k}}{(2k)!} > 0$$

where B_k is the k-th Bernoulli number :

$$\frac{t}{e^t-1}=\sum_{n\geqslant 0}\frac{B_n}{n!}t^n.$$

Consequently we have

$$\tilde{G_{2k}}(q)=\frac{2(2\pi i)^{2k}}{(2k-1)!}\left(-\frac{B_{2k}}{2(2k)}+\sum_{n\geqslant 1}\sigma_{2k-1}(n)q^n\right)\in(2\pi i)^{2k}\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}[\![q]\!].$$

The discriminant of the polynomial $4X^3-g_4(\tau)X-g_6(\tau)$ is an homogeneous polynomial in the coefficients, so that it gives us a modular form of weight 12. More precisely it is defined by

$$\Delta(\tau):=-(-g_4(\tau))^3-27(-g_6(\tau))^2=60^3G_4(\tau)^3-27\cdot 140^2G_6(\tau)^2).$$

Using the values $B_4=-1/30$ and $B_6=1/42$, we obtain

$$\tilde{\Delta}(q)=(2\pi)^{12}(q+\tau(2)q^2+\tau(3)q^3+\cdots)\in(2\pi i)^{12}(\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}[\![q]\!]).$$

Actually we have $(2\pi)^{-12}\tilde{\Delta}\in q\mathbb{Z}[\![z]\!]$. Namely, we have

$$2^6\cdot 3^3(2\pi)^{-12}\tilde{\Delta}=(1+2^4\cdot 3\cdot 5A(q))^3-(1-2^3\cdot 3^2\cdot 7B(q))^2$$

with $A(q)=\sum_{n\geqslant 1}\sigma_3(n)q^n$ and $B(q)=\sum_{n\geqslant 1}\sigma_5(n)q^n$. However it is easy to check that $12\mid 5\sigma_3(n)+7\sigma_5(n)$ for all $n\geqslant 1$. Consequently

$$2^6\cdot 3^3(2\pi)^{-12}\tilde{\Delta}\equiv 2^4\cdot 3^2\cdot 5A(q)+2^4\cdot 3^2\cdot 7B(q)\equiv 0\,[2]^6\cdot 3^3.$$

The rational numbers $\tau(n)$ are actually integers and are called Ramanujan numbers. They have fascinating arithmetic properties. Among them are

- If $m\wedge n=1$, then $\tau(mn)=\tau(m)\tau(n)$;
- for p a prime number, and $n\geqslant 1$, $\tau(p)\tau(p^n)=\tau(p^{n+1})+p^{11}\tau(p^{n-1})$;
- for p a prime number, $|\tau(p)|<2p^{11/2}$;
- for p a prime number, $p\neq 691$, we have $\tau(p)\equiv 1+p^{11}\,[6]91\ldots$

This type of arithmetic properties are shared by lots of other functions which are called *modular forms*.

Proposition 1.9. *For $\tau\in\mathbb{H}$, we have $\Delta(\tau)\neq 0$.*

Proof. Let $\tau \in \mathbb{H}$. We know that the function $\mathfrak{p}'$ vanishes at the points of $\frac{1}{2}\Lambda_\tau \smallsetminus \Lambda_\tau$. If z is such a point, then $\mathfrak{p}(z)$ is a zero of $4X^3 - g_4(\tau)X - g_6(\tau)$. Consequently, in order to prove that $\Delta(\tau)$, it is sufficient to prove that $\mathfrak{p}$ takes pairwise distinct values on

$$\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$$

where (ω_1, ω_2) is a basis of Λ_τ. If ω is one of these values, it is sufficient to show that the elliptic function $\mathfrak{p} - \mathfrak{p}(\omega)$ has only one zero. That is a consequence of the fact that, since $\mathfrak{p}'(\omega) = 0$, ω is at least a double zero of $\mathfrak{p}$ and of the equality $\deg(\mathfrak{p} - \mathfrak{p}(\omega)) = 2$. □

We can consequently define

$$j(\Lambda) \coloneqq \frac{1728 g_4(\Lambda)^3}{\Delta(\Lambda)}$$

and $j(\tau) \coloneqq j(\Lambda_\tau)$. This is a weakly modular form of weight 0, that is an holomorphic function on $\mathbb{H}$ invariant under the action of $\mathbb{H}$. Moreover, we have $1728\tilde{g_4} \in 1 + q\mathbb{Z}[\![q]\!]$ so that

$$\tilde{j}(q) = \frac{1}{q} + \sum_{n \geqslant 0} c_n q^n \in \frac{1}{q} + \mathbb{Z}[\![q]\!]. \tag{2}$$

Consequently j is a meromorphic modular form of weight 0.

Let $\mathcal{D} = \{z \in \mathbb{H} \mid |\operatorname{Re} z| \leqslant 1,\ \ |z| \geqslant 1\}$.

Theorem 1.10. *We have* $\mathbb{H} = \bigcup_{g \in \mathrm{SL}_2(\mathbb{Z})} g\mathcal{D}$.

Proof. If $z \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we have $\operatorname{Im}\gamma(z) = (cz+d)^{-1} \operatorname{Im} z$. The set of elements of the form $cz + d$ with $(c, d) \in \mathbb{Z}^2$ is a lattice of of $\mathbb{C}$, which implies that the set $\{(cz+d)^{-1} \mid (c,d) \in \mathbb{Z}^2\} \smallsetminus \{(0,0)\}$ is bounded. Consequently we can find some $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\operatorname{Im}\Gamma_0(z)$ is maximal. The element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ on $\mathbb{H}$ preserves imaginary part. Consequently we can find $n \in \mathbb{Z}$ such that, for $\gamma_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n \gamma_0$, $\operatorname{Im}\gamma_1(z)$ is maximal and $|\operatorname{Re}\gamma_1(z)| \leqslant 1$. Let $\gamma_2 \coloneqq \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\gamma_1$. We have $|\gamma_2(z)| = |\gamma_1(z)|^{-1}$. By maximality, we conclude that $|\gamma_1(z)| \geqslant |\gamma_1(z)|^{-1}$ which implies $|\gamma_1(z)| \geqslant 1$. We have $\mathbb{H} = \bigcup_{\gamma \in \mathrm{SL}_2(\mathbb{Z})} \gamma(\mathcal{D})$. □

Corollary 1.11. *The modular forms of weight* 0 *are the constant functions on* $\mathbb{H}$.

Proof. Let f be a modular form of weight 0. Up to translating f by a constant function, we can assume that $\tilde{f}(0) = 0$. We deduce from this fact that and from Theorem 1.10 that is reaching is maximum on a compact of $\mathcal{F}$. It follows from the maximum principle that f is constant. □

Corollary 1.12. *The function j is surjective, ie $j(\mathbb{H}) = \mathbb{C}$.*

Proof. Let $c \in \mathbb{C}$. Assume that there is a no $\tau \in \mathbb{H}$ such that $j(\tau) = c$. The modular form $g_4^3 - c\Delta$ does not vanish on $\mathbb{H}$. As $\zeta(4) > 0$, we deduce that the function $\frac{g_4^3}{g_4^3 - c\Delta}$ is a modular form of weight 0 and consequently is constant. Hence there exists $d \in \mathbb{C}$ such that $g_4^3 = d(g_4^3 - c\Delta)$ and $(1 - d + dc)g_4^3 = 27dcg_6^2$. We can check that g_4^3 and g_6^2 are not colinear, consequently $dc = 1 - d + dc = 0$ and $d = 1$, $c = 0$. However $j(e^{\frac{2\pi i}{3}}) = 0$. □

2 Modular curves as Riemann surfaces

2.1 Properly discontinuous actions on locally compact spaces

In this course, a *locally compact topological space* is a topological which is Hausdorff and such that each point has a basis of neighbourhoods made of compact subsets. An action of a group on a topological space is an action of group on the underlying set by continuous (and hence bicontinuous) transformations. Topological groups will always assumed to be Hausdorff.

Let X be a locally compact topological space and let Γ be a topological group acting continuously on X. We say Γ acts *properly* on X if the map $\Gamma \times X \to X \times X$ defined by $(g, x) \mapsto (x, g \cdot x)$ is proper, ie such that the inverse image of a compact subset is compact. It is equivalent to ask that for each pair (K_1, K_2) of compact subsets of X, the subset $\{\gamma \in \Gamma,\ K_1 \cap \gamma(K_2) \neq \emptyset\}$ is compact. As a consequence, the graph of the action is closed in $X \times X$, which implies that the topological space $\Gamma\backslash X$ is Hausdorff. In the particular case where Γ is a discrete group, it acts properly if and only if for each pair (K_1, K_2) of compact subsets of X, the subset $\{\gamma \in \Gamma,\ K_1 \cap \gamma(K_2) \neq \emptyset\}$ is finite.

Proposition 2.1. *Let Γ be a discrete group acting properly on X. For a pair (x, y) of points of X such that $x \neq y$, there exist open neighbourhoods U and V of x and y such that*

$$\{\gamma \in \Gamma \mid \gamma(U) \cap V \neq \emptyset\} = \{\gamma \in \Gamma \mid \gamma(x) = y\}.$$

Moreover for all $x \in X$, the stabilizer Γ_x of x is finite.

Proof. Let K_1 and K_2 be compact neighbourhoods of x and y. Let E be the finite set of elements $\gamma \in \Gamma$ such that $\gamma(K_1) \cap K_2 \neq \emptyset$ and $\gamma(x) \neq y$. Since X is Hausdorff, we can find, for $\gamma \in E$ some open subsets $U_\gamma \subset K_1$ and $V_\gamma \subset K_2$ such that $\gamma(U_\gamma) \cap V_\gamma = \emptyset$, $x \in U_\gamma$ and $y \in V_\gamma$. Let $U = \cap_{\gamma \in E} U_\gamma$ and $V = \cap_{\gamma \in E} V_\gamma$. If $\gamma(U) \cap V \neq \emptyset$, then $\gamma(K_1) \cap K_2 \neq \emptyset$. As $\gamma(U_\gamma) \cap V_\gamma \neq \emptyset$ for $\gamma \in E$, we must have $\gamma(x) = y$. The last assertion is plain. □

Corollary 2.2. *If Γ is a discrete group acting properly and freely on X, then the quotient map $\pi : X \to \Gamma\backslash X$ is a topological covering of group Γ.*

Proof. Let $y \in \Gamma\backslash X$ and $x \in X$ such that $\pi(x) = y$. It follows from Proposition 2.1 that there exists an open subset $U \subset X$ containing x such that $U \cap \gamma(U) \neq \emptyset \Rightarrow \gamma = e$.

This implies that the restriction of π to U induces a continuous bijection from U to $V \coloneqq \pi(U)$. As π is open, V is an open subset of $\Gamma\backslash X$ containing y and $\pi\mid_U$ is an homeomorphism from U to V. Finally we have $\pi^{-1}(V) = \coprod_{\gamma\in\Gamma}\gamma(U)$, which implies that π is a topological covering of group Γ. □

The following situation produces examples and of properly actions of discrete groups. Let G be a locally compact topological group. It acts on itself on the right by $(g,h)\mapsto hg^{-1}$. As the corresponding map $(g,h)\mapsto(g,hg^{-1})$ is an homeomorphism of $G\times G$ on itself, this action is proper and so is the action of any closed subgroup $K\subset G$ of G on G. Let $X \coloneqq G/K$. Consequently the space X is Hausdorff and, the projection map $\pi : G\mapsto G/K$ being open, X is locally compact. The group G acts continuously on X via $(g,hK)\mapsto ghK$.

Lemma 2.3. *A subset $A\subset G/K$ is compact if and only if there exists a compact subset $B\in G$ such that $\pi^{-1}(A) = BK$. If moreover K is compact, then the projection $\pi : G\to G/K$ is proper, ie $A\subset G/K$ is compact if and only if $\pi^{-1}(A)$ is compact.*

Proof. The map π is continuous and if $\pi^{-1}(A) = BK$, then $A = \pi(B)$. Consequently if B is compact, then A is compact. Conversely assume that A is compact. Let $(U_i)_{i\in I}$ be some open covering of $\pi^{-1}(A)$ such that each $\overline{U_i}$ is compact. Then $(\pi(U_i))_{i\in I}$ is an open covering of A and we can find some finite subset $J\subset I$ such that $A = \bigcup_{i\in J}\pi(U_i)$. Let $B = \bigcup_{i\in J}\overline{U_i}$. By continuity of π, we have $\pi(B) = A$ so that $\pi^{-1}(A) = BK$. The last assertion follows immediately. □

Corollary 2.4. *Let G be a locally compact topological group and let $K\subset G$ be some compact subgroup. Then every closed subgroup of G acts properly on G/K. In particular every discrete subgroup of G acts properly on G/K.*

Proof. It is sufficient to prove that G acts properly on G/K. Let $\pi : G\to G/K$ be the projection map. As K is compact, the map π is proper. Let K_1 and K_2 be compact subsets of G/K. Then

$$\{g\in G \mid g(K_1)\cap K_2\neq\emptyset\} = G\cap\pi^{-1}(K_2)\pi^{-1}(K_1)^{-1}$$

is compact. The last assertion comes from the fact that a discrete subgroup of G is closed in G. □

2.2 Quotients of Poincaré upper half plane

Let $G = \mathrm{SL}_2(\mathbb{R})$, $X = \mathbb{H} = \{\tau\in\mathbb{C},\,\mathrm{Im}\,\tau > 0\}$. Then G acts continuously on $\mathbb{H}$ via homographies

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\cdot\tau = \frac{a\tau+b}{c\tau+d}.$$

The action is transitive since $x+iy = \left(\begin{smallmatrix} y^{1/2} & y^{-1/2}x \\ 0 & y^{-1/2} \end{smallmatrix}\right)$ and the stabilizer of i is the compact subgroup $K = \mathrm{SO}_2(\mathbb{R})$. Consequently there is a G-equivariant continuous bijection

$$G/K \to \mathbb{H}.$$

It is actually an isomorphism since it has a continuous section given by

$$x + iy \mapsto \left(\begin{smallmatrix} y^{1/2} & y^{-1/2}x \\ 0 & y^{-1/2} \end{smallmatrix}\right).$$

Consequently each discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{R})$ acts properly on $\mathbb{H}$ and the quotient $\Gamma\backslash\mathbb{H}$ is separated. Note that the action of $\mathrm{SL}_2(\mathbb{R})$ is the restriction to $\mathrm{SL}_2(\mathbb{R})$ of an action of $\mathrm{GL}_2(\mathbb{C})$ on the projective line $\mathbb{P}^1(\mathbb{C})$ in which $\mathbb{H}$ is embedded via $\tau \mapsto (\tau : 1)$. The kernel of the action is the center $\{\pm I_2\}$ of $\mathrm{SL}_2(\mathbb{R})$. This suggests to introduce the following notation : if Γ is a subgroup of $\mathrm{SL}_2(\mathbb{R})$, we define $\overline{\Gamma}$ its image in $\mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$.

Let $\sigma \in \mathrm{SL}_2(\mathbb{R}) \smallsetminus \{\pm I_2\}$. We say that σ is *elliptic* if it has two (conjugated) eigenvalues in $\mathbb{C} \smallsetminus \mathbb{R}$, it is *hyperbolic* if has two different real eigenvalues and *parabolic* in the last case, ie. if it has a unique real eigenvalue.

Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. An element $\tau \in \mathbb{H}$ is an *elliptic point* of Γ if it is fixed by an elliptic element of Γ. An element $c \in \mathbb{P}^1(\mathbb{R})$ is called a *cusp* of Γ if it is fixed by a parabolic element of Γ.

Proposition 2.5. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be some discrete subgroup.*

(i) Let $\tau \in \mathbb{H}$ be an elliptic point of Γ. Then the stabilizer Γ_τ of τ in Γ is a finite cyclic group.

(ii) Let $c \in \mathbb{P}^1(\mathbb{R})$ be a cusp of Γ and let Γ_c be the stabilizer of Γ. Then the quotient group $\Gamma_c/\Gamma_c \cap \{\pm I_2\}$ is isomorphic to $\mathbb{Z}$ and the elements of $\Gamma_c \smallsetminus \{\pm I_2\}$ are all parabolic.

Proof. The first point comes from the fact that the stabilizer of a point of $\mathbb{H}$ is conjugated to a discrete subgroup of the stabilizer of i in $\mathrm{SL}_2(\mathbb{R})$. This stabilizer is $\mathrm{SO}_2(\mathbb{R})$ which is isomorphic to the circle $\mathbb{R}/\mathbb{Z}$ whose discrete subgroups are finite cyclic.

The group $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathbb{P}^1(\mathbb{R})$. We can choose $\sigma \in \mathrm{SL}_2(\mathbb{R})$ such that $\sigma(\infty) = c$ and then $\Gamma_c = \sigma\Gamma_\infty\sigma^{-1}$. A direct computation shows that $\mathrm{SL}_2(\mathbb{R})_\infty = \{\pm I_2\} \times \left(\begin{smallmatrix} 1 & \mathbb{R} \\ 0 & 1 \end{smallmatrix}\right)$. Consequently $\mathrm{SL}_2(\mathbb{R})_c/\{\pm I_1\} \simeq \mathbb{R}$ and $\Gamma_c/\Gamma_c \cap \{\pm I_2\}$ is isomorphic to a subgroup of $\mathbb{R}$. Let $P(c) \subset \mathrm{SL}_2(\mathbb{R})$ be the subgroup generated by the parabolic elements fixing c. Then

$$P(c) = \sigma\left\{\pm\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R}\right\}\sigma^{-1}.$$

Moreover Γ_c, and consequently $P(c) \cap \Gamma$, is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})_c$ so that $(P(c)\cap\Gamma)/(\Gamma\cap\{\pm I_2\})$ identifies to a discrete subgroup of $\mathbb{R}$. By assumption, $(P(c)\cap\Gamma) \not\subset \{\pm I_2\}$ so that $(P(c)\cap\Gamma)/(\Gamma \cap \{\pm I_2\}) \simeq \mathbb{Z}$. If Γ_c contains non central elements which are not parabolic, they are necessarily hyperbolic. Assume that there exists some hyperbolic

element $\rho \in \Gamma_c$. We have $\rho = \sigma \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \sigma^{-1}$ for some $a \in \mathbb{R}^\times$ and $b \in \mathbb{R}$. Since ρ is not parabolic, we must have $|a| \neq 1$ and, up to exchanging ρ and ρ^{-1}, we can assume that $0 < |a| < 1$. Let $\theta \in P(c) \cap \Gamma$ be a generator of $(P(c) \cap \Gamma)/(\Gamma \cap \{\pm I_2\})$. Then $\theta = \pm\sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1}$ with $h \neq 0$. Then we have

$$\rho\theta\rho^{-1} = \pm\sigma \begin{pmatrix} 1 & a^2 h \\ 0 & 1 \end{pmatrix} \sigma^{-1} \in P(c).$$

As $|a^2 h| < |h|$, we obtain a contradiction with the fact that θ generates $(P(c) \cap \Gamma)/(\Gamma \cap \{\pm I_2\})$. □

If $\tau \in \mathbb{H}$ is an elliptic point of Γ, the *order* of this elliptic point is the cardinal of the cyclic group $\Gamma_\tau / \Gamma_\tau \cap \{\pm I_2\}$.

We say that two subgroups Γ and Γ' of $\mathrm{SL}_2(\mathbb{R})$ are *commensurable* if the intersection $\Gamma \cap \Gamma'$ is of finite index in both Γ and Γ'. If Γ and Γ' are commensurable, then Γ is discrete if and only if Γ' is discrete. In this case, it follows from the proposition these two subgroups have the same set of cusps. However they can have different elliptic points.

The group $\mathrm{SL}_2(\mathbb{Z})$ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. We say that a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ is an *arithmetic subgroup* if it is commensurable to $\mathrm{SL}_2(\mathbb{R})$.

Proposition 2.6. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be an arithmetic subgroup. Then its set of cusps is exactly $\mathbb{P}^1(\mathbb{Q})$.*

Proof. We know that the set of cusps of Γ is the set of cusps of $\mathrm{SL}_2(\mathbb{Z})$. As $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is a parabolic element of $\mathrm{SL}_2(\mathbb{Z})$ fixing ∞, the point ∞ is a cusp of $\mathrm{SL}_2(\mathbb{Z})$. Moreover the orbit of ∞ under the action of $\mathrm{SL}_2(\mathbb{Z})$ is exactly $\mathbb{P}^1(\mathbb{Q})$ so that all points of $\mathbb{P}^1(\mathbb{Q})$ are cusps. Conversely if $c \neq \infty$ is a cusp for $\mathrm{SL}_2(\mathbb{Z})$, let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be some parabolic element fixing c. Then c is a root of the non separable polynomial $cx^2 + (d-a)x - b = 0$ so that c is a rational number. □

2.3 Other examples of arithmetic quotients

We can consider the case of the connected Lie group $G = \mathrm{SL}_n(\mathbb{R})$, $K = \mathrm{SO}_n(\mathbb{R})$ and $\Gamma = \mathrm{SL}_n(\mathbb{Z})$. Then the group Γ acts properly on the topological space $X \coloneqq G/K$. Using polar decomposition we can check that the space X is homeomorphic to the space of symmetric matrices of trace 0 in $\mathcal{M}_n(\mathbb{R})$.

Here is an other example. Let $G = U(n-1,1)(\mathbb{R})$ be the unitary group of the hermitian form $q(z_1, \ldots, z_n) = \sum_{i=1}^{n-1} |z_i|^2 - |z_n|^2$ on $\mathbb{C}^n$ and $K = U(n-1)(\mathbb{R}) \times U(1)(\mathbb{R})$ the subgroup of element preserving the line $\mathbb{C}e_n$. The subgroup $\Gamma \coloneqq \mathrm{GL}_n(\mathbb{Z}) \cap U(n-1,1)(\mathbb{R})$ is a discrete subgroup of G and it acts properly on $X \coloneqq G/K$. The space is X is now homeomorphic to the open unit disc in $\mathbb{C}^{n-1}$ the map being defined by $g \mapsto (z_1, \ldots, z_{n-1})$ where $ge_n = z_n \left(\sum_{i=1}^{n-1} z_i e_i + e_n \right)$. The space X/K has a natural structure of complex analytic space and the action of elements of G on it is by holomorphic transformations.

2.4 Elliptic points for $\mathrm{SL}_2(\mathbb{Z})$

Lemma 2.7. *Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ be a torsion element. Then γ is $\pm I_2$ or has order 4 and characteristic polynomial X^2+1 or has order 3 and characteristic polynomial X^2+X+1 or has order 6 and characteristic polynomial X^2-X+1. Moreover γ has order 6 if and only if $-\gamma$ has order 3.*

Proof. The eigenvalues of γ are roots of unity. As $\det\gamma = 1$, 1 is an eigenvalue of γ if and only if $\gamma = I_2$ and -1 is an eigenvalue of γ if and only if $\gamma = -I_2$. We can assume that the eigenvalues of γ are different from 1 and -1 so that $|\mathrm{Tr}\,\gamma| < 2$. This implies that the characteristic polynomial of γ is either X^2+1 or $X^2 \pm X + 1$. The rest follows. □

Lemma 2.8. *Two torsion elements of $\mathrm{SL}_2(\mathbb{Z})$ are conjugated inside $\mathrm{GL}_2(\mathbb{Z})$ if and only if they have the same characteristic polynomial.*

Proof. Let γ_1 and γ_2 be two torsion element having the same characteristic polynomial. They have consequently the same order and we can assume they are both different from $\pm I_2$. They generate isomorphic subrings $A_1 \coloneqq \mathbb{Z}[\gamma_1]$ and $A_2 \coloneqq \mathbb{Z}[\gamma_2]$ of $\mathcal{M}_2(\mathbb{Z})$ which are isomorphic either to $\mathbb{Z}[X]/(X^2+1)$ or to $\mathbb{Z}[X]/(X^2+X+1)$. As a consequence they generate isomorphic principal rings. Let θ be the unique isomorphism from A_1 to A_2 sending γ_1 onto γ_2. The group $\mathbb{Z}^2$ carries two structures of A_1-module. The first one comes from the inclusion $A_1 \subset \mathcal{M}_2(\mathbb{Z})$ and the second one from the composite of θ with the inclusion $A_2 \subset \mathcal{M}_2(\mathbb{Z})$. Since A_1 is a finite free $\mathbb{Z}$-module of rank 2, for both structures of A_1-modules, $\mathbb{Z}^2$ is a projective A_1-module of rank 1. As A_1 is principal, for both structures of A_1-modules, $\mathbb{Z}^2$ is a free A_1-module of rank 1. Thus both structures of A_1-module on $\mathbb{Z}^2$ are isomorphic which implies that there exists $M \in \mathrm{GL}_2(\mathbb{Z})$ such that $M\gamma_1 M^{-1} = \gamma_2$. □

Lemma 2.9. *Let γ be an elliptic element of $\mathrm{SL}_2(\mathbb{Z})$. Then γ and γ^{-1} are not conjugated in $\mathrm{SL}_2(\mathbb{Z})$. If γ_1 and γ_2 are two elements of $\mathrm{SL}_2(\mathbb{Z})$ having the same characteristic polynomial, then γ_1 and γ_2 are conjugated in $\mathrm{SL}_2(\mathbb{Z})$ or γ_1 and γ_2^{-1} are conjugated in $\mathrm{SL}_2(\mathbb{Z})$.*

Proof. Assume that γ and γ^{-1} are conjugated in $\mathrm{SL}_2(\mathbb{Z})$. In particular they are conjugated in $\mathrm{SL}_2(\mathbb{R})$. As γ is elliptic, γ has a fixed point in $\mathbb{H}$. Up to conjugation by an element of $\mathrm{SL}_2(\mathbb{R})$, we can assume that γ fixes i and $\gamma \in \mathrm{SO}_2(\mathbb{R})$. Then γ and γ^{-1} are two elements which are conjugated by an element of $\mathrm{SL}_2(\mathbb{R})$. This implies that they have the same oriented angle, which is consequently in $\pi\mathbb{Z}$. This implies $\gamma = \pm I_2$ contradicting the fact that γ is elliptic. Now assume that γ_1 and γ_2 have the same characteristic polynomial. Then there exists $P \in \mathrm{GL}_2(\mathbb{Z})$ such that $\gamma_2 = P\Gamma_1 P^{-1}$. If $\det(P) = 1$, we are done. If not, γ_1 and γ_1^{-1} are elliptic element having the same order. They have consequently conjugated in $\mathrm{GL}_2(\mathbb{Z})$ by a matrix of determinant -1. This implies that γ_2 and γ_1^{-1} are conjugated in $\mathrm{SL}_2(\mathbb{Z})$. □

Corollary 2.10. *Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ be an elliptic element. Then either*

(i) the element γ has order four and is conjugated in $\mathrm{SL}_2(\mathbb{Z})$ to $S \coloneqq \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ or to $S^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. As a consequence its characteristic polynomial is $X^2 + 1$;

(ii) the element γ has order 3 or 6. If it has order 3, it is conjugated in $\mathrm{SL}_2(\mathbb{Z})$ to $T \coloneqq \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ or to $T^{-1} = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. If it has order 6, then $-\gamma$ has order 3 and is conjugated in $\mathrm{SL}_2(\mathbb{Z})$ to T or T^{-1}.

Moreover there are exactly two $\mathrm{SL}_2(\mathbb{Z})$ orbits of elliptic points in $\mathbb{H}$. One of them consists of the elliptic points of order 2 and the other one of the elliptic points of order 3.

2.5 Compactifications

We fix $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ a discrete subgroup and define $\mathbb{H}^*$ the union of $\mathbb{H}$ and of the set of cups of Γ. Even if the notation do *not* suggest it, it really depends on Γ.

Example 2.11. If Γ is an arithmetic subgroup, we have $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

We define a topology on $\mathbb{H}^*$. For $r > 0$, let $U_{\infty,r} = \{z \in \mathbb{H},\, \mathrm{Im}\, z > r\} \cup \{\infty\}$ and, if $c \in \mathbb{R}$ is a cusp of Γ, let $U_{c,r} = \{z \in \mathbb{H},\, |z - (c + ir)| < r\} \cup \{c\}$. Let $\mathcal{T}$ be the set of all open subsets of $\mathbb{H}$ and let

$$\mathcal{T}^* \coloneqq \mathcal{T} \cup \bigcup_{c \in \mathbb{H}^* \smallsetminus \mathbb{H}} \{U_{c,r} \mid r > 0\}.$$

Lemma 2.12. *The set $\mathcal{T}^*$ is a basis of open neighbourhoods of a unique topology of $\mathbb{H}^*$. Moreover $\mathbb{H}$ is open in $\mathbb{H}^*$ and a subset of $\mathbb{H}$ is open in $\mathbb{H}^*$ if and only if it is open in $\mathbb{H}$.*

Proof. The set $\mathcal{T}^*$ is stable under finite intersections. □

The action of Γ on $\mathbb{H}^*$ is continuous.

Theorem 2.13. *The topological space $\Gamma\backslash\mathbb{H}^*$ is locally compact.*

Proof. Let $\pi_\Gamma : \mathbb{H}^* \to \Gamma\backslash\mathbb{H}^*$ be the projection. It is an open map which implies that $Y(\Gamma) = \pi_\Gamma(\mathbb{H}) \subset X(\Gamma)$ is an open subset which is already known to be Hausdorff. Consequently in order to prove that $X(\Gamma)$ it is sufficient to prove that, for $x \in X(\Gamma) \smallsetminus Y(\Gamma)$ and $y \in X(\Gamma) \smallsetminus \{x\}$ we can find disjoint open subsets U and V such that $x \in U$ and $y \in V$. The following lemmas will be useful :

Lemma 2.14. *Assume that ∞ is a cusp of Γ. Then there exists $r > 0$ such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \smallsetminus \Gamma_\infty$, we have $|c| \geqslant r$. Moreover, for all $\gamma \in \Gamma \smallsetminus \Gamma_\infty$ and for all $\tau \in \mathbb{H}$, we have $\mathrm{Im}\, \tau\, \mathrm{Im}\, \gamma(\tau) \leqslant 1/r^2$.*

Proof. Let $h > 0$ such that $t_h \coloneqq \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_\infty$. We fix $M \geqslant 0$. Assume that $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \setminus \Gamma_\infty$ such that $|c| \leqslant M$. Let $n \in \mathbb{Z}$ such that $1 \leqslant d + nhc \leqslant 1 + h|c| \leqslant 1 + hM$ and $m \in \mathbb{Z}$ such that $|\operatorname{Re} \gamma t_h^n(i)| \leqslant \frac{h}{2}$. If $\gamma_1 = t_h^m \gamma t_h^n = \left(\begin{smallmatrix} * & * \\ c & d+hnc \end{smallmatrix}\right)$, we have

$$\operatorname{Im} \gamma_1(i) = \operatorname{Im} \gamma t_h^n(i) = \frac{1}{|c|^2 + |d + hnc|^2}$$

so that $\gamma_1(i) \in K$ where K is the compact

$$K = \left\{ \tau \in \mathbb{H} \mid \frac{1}{(1+hM)^2 + M^2} \leqslant \operatorname{Im} \tau \leqslant 1, \, |\operatorname{Re} \tau| \leqslant \frac{h}{2} \right\}.$$

As Γ acts properly on $\mathbb{H}$, the set $\{\sigma \in \Gamma \mid \sigma(i) \in K\}$ is finite, so that the number of possible $|c| \leqslant M$ is finite. Therefore there exists $r > 0$ such that $|c| \geqslant r$ as soon as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \setminus \Gamma_\infty$.

Consequently if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \setminus \Gamma_\infty$ and $\tau \in \mathbb{H}$, we have

$$\operatorname{Im} \gamma(\tau) \operatorname{Im} \tau = \frac{(\operatorname{Im} \tau)^2}{|c\tau + d|^2} \leqslant \frac{(\operatorname{Im} \tau)^2}{|c|^2 (\operatorname{Im} \tau)^2} \leqslant \frac{1}{|c|^2} \leqslant \frac{1}{r^2}.$$

□

Let $c \in \mathbb{P}^1(\mathbb{R})$ such that $\pi_\Gamma(c) = x$ and let $\sigma \in \mathrm{SL}_2(\mathbb{R})$ such that $\sigma(\infty) = c$. The group $\sigma\Gamma\sigma^{-1}$ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ and the map $\tau \mapsto \sigma(\tau)$ induces an homeomorphism of $X(\sigma\Gamma\sigma^{-1})$ onto $X(\Gamma)$. Up to changing Γ into $\sigma\Gamma\sigma^{-1}$ and x into $\pi_{\sigma\Gamma\sigma^{-1}}(\infty)$, we can assume that $x = \pi_\Gamma(\infty)$ and that ∞ is a cusp of Γ.

Suppose first that $y \in Y(\Gamma)$. Then $y = \pi_\Gamma(\tau_0)$ for some $\tau_0 \in \mathbb{H}$. Let $r > 0$ be like in Lemma 2.14. Let $K \subset \mathbb{H}$ be some compact neighbourhood of τ_0. There exists some real numbers $0 < A \leqslant B$ such that

$$K \subset \{\tau \in \mathbb{H} \mid A \leqslant \operatorname{Im} \tau \leqslant B\}.$$

Let $U \coloneqq \{\tau \in \mathbb{H} \mid \operatorname{Im} \tau > \max(B, 1/Ar^2)\} \cup \{\infty\}$. Then U is an open neighbourhood of ∞ in $\mathbb{H}^*$. If $\gamma \in \Gamma_\infty$, we have $\operatorname{Im} \gamma(\tau) = \operatorname{Im} \tau$ for all $\tau \in \mathbb{H}$, so that $\gamma(K) \cap U = \emptyset$. If $\gamma \in \Gamma \setminus \Gamma_\infty$, it follows from Lemma 2.14 that $\operatorname{Im} \tau \operatorname{Im} \gamma(\tau) \leqslant 1/r^2$ for $\tau \in \mathbb{H}$ so that $\operatorname{Im} \gamma(\tau) < B$ if $\tau \in K$. This proves that $\gamma(K) \cap U = \emptyset$. Consequently we have $\pi_\Gamma(\mathring{K}) \cap \pi_\Gamma(U) = \emptyset$ and $\pi_\Gamma(\mathring{K})$ and $\pi_\Gamma(U)$ are disjoint open neighbourhoods of y and x in $X(\Gamma)$.

Suppose now that $y \neq x$ is a cusp of $X(\Gamma)$ so that $y = \pi_\Gamma(x)$ for some cusp c of Γ. We have $\Gamma c \neq \Gamma\infty$. Fix $u > 0$ and $L_u \coloneqq \{\tau \in \mathbb{H} \mid \operatorname{Im} \tau = u\}$. Let $h > 0$ be such that the matrix $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and set $K \coloneqq \{\tau \in L_u \mid 0 \leqslant \operatorname{Re} \tau \leqslant h\}$ and $V \coloneqq \{\tau \in \mathbb{H} \mid \operatorname{Im} \tau > u\}$. The space K is compact and contained in $\mathbb{H}$. Using the previous case, we can consequently find some open neighbourhood U of c in $\mathbb{H}^*$ such that $K \cap \Gamma U = \emptyset$. We can assume that U of the form $U_{c,s}$ for some real $s > 0$.

Assume that there exists $\gamma \in \Gamma$ such that $\gamma(U) \cap V \neq \emptyset$. Since U is connected, we have $\gamma(U) \cap L_u \neq \emptyset$. We can find $\gamma' \in \Gamma_\infty$ such that $\gamma'\gamma(U) \cap K \neq \emptyset$, which is a contradiction.

Finally we have to prove that each element of $X(\Gamma)$ has a compact neighbourhood. It is sufficient to prove that each $\tau \in \mathbb{H}^*$, there exists a compact subset $K \subset \mathbb{H}^*$ containing τ such that $\pi_\Gamma(K)$ is a neighbourhood of $\pi_\Gamma(\tau)$ in $X(\Gamma)$. If $\tau \in \mathbb{H}$, it is a consequence of the local compactness of $\mathbb{H}$. We can consequently assume that τ is a cusp of Γ and, up to conjugating Γ in $\mathrm{SL}_2(\mathbb{R})$, that τ is ∞. Let $r > 0$ and let $U \coloneqq \{\tau \in \mathbb{H} \mid \operatorname{Im}\tau \geqslant r\} \cup \{\infty\}$. Then U is a neighbourhood of ∞ in $\mathbb{H}^*$ so that $\pi_\Gamma(U)$ is a neighbourhood of $\pi_\Gamma(\infty)$ in $X(\Gamma)$. Let $h > 0$ be such that the matrix $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and

$$K \coloneqq \{\tau \in \mathbb{H} \mid \operatorname{Im}\tau \geqslant r,\, 0 \leqslant \operatorname{Re}\tau \leqslant h\} \cup \{\infty\}.$$

We have $U \subset \Gamma K$ so that $\pi_\Gamma(U) \subset \pi_\Gamma(K)$ and $\pi_\Gamma(K)$ is a neighbourhood of $\pi_\Gamma(\Gamma)$. Now K is a compact subset of $\mathbb{H}^*$. Namely if $(U_i)_{i\in I}$ is an open covering of K. There exists i_0 such that U_{i_0} is a neighbourhood of ∞ meaning that there exists $r' \geqslant r$ such that $U_{\infty,r'} \cap K \subset U_{i_0}$. This implies that

$$\{\tau \in \mathbb{H} \mid r \leqslant \operatorname{Im}\tau \leqslant r'\, 0 \leqslant \operatorname{Re}\tau \leqslant h\} \subset \bigcup_{i\neq i_0} U_i$$

and the left hand side is a compact space, consequently there exists a finite subset $J \subset I \smallsetminus \{i_0\}$ such that $K \subset U_{i_0} \bigcup_{i\in J} U_i$. This proves that K is a compact subset of $\mathbb{H}^*$. □

2.6 Complex structures

If $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ is a discrete subgroup, we use the following notation

$$Y(\Gamma) \coloneqq \Gamma\backslash\mathbb{H},\ X(\Gamma) \coloneqq \Gamma\backslash\mathbb{H}^*.$$

The elements of $X(\Gamma) \smallsetminus Y(\Gamma)$ are called the *cusps* of $X(\Gamma)$ and the images in $Y(\Gamma)$ of elliptic points of Γ are called the *elliptic points* of $X(\Gamma)$.

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a discrete subgroup. Let $\mathcal{O}_\mathbb{H}$ be the sheaf of holomorphic functions on $\mathbb{H}$. We note $\mathcal{O}_{\mathbb{H}^*}$ the sheaf of holomorphic functions on $\mathbb{H}$ which extend to continuous functions over $\mathbb{H}^*$. More precisely if $U \subset \mathbb{H}^*$ is an open subset, we set $\mathcal{O}_{\mathbb{H}^*}(U)$ the set of functions $f \in \mathcal{O}_\mathbb{H}(U \cap \mathbb{H})$ such that, for all cusp $c \in U$, the restriction of f to some (or equivalently any) $U_{c,r}$ for $r > 0$ has a limit at c, for the topology induces by $\mathbb{H}^*$. Note that this is not the topology induced by $\mathbb{H}$ when $c \neq \infty$. It can be easily checked that $\mathcal{O}_{\mathbb{H}^*}$ is the subsheaf of the direct image of the sheaf of holomorphic functions $\mathcal{O}_\mathbb{H}$ by the inclusion $j : \mathbb{H} \subset \mathbb{H}^*$. Namely this is the intersection of $j_*\mathcal{O}_\mathbb{H}$ with the sheaf of continuous functions on $\mathbb{H}^*$ inside the sheaf of all functions on $\mathbb{H}^*$.

Let π_Γ be the quotient map $\mathbb{H}^* \to X(\Gamma)$. We define a sheaf on the quotient space $X(\Gamma)$ by the formula

$$\mathcal{O}_{X(\Gamma)} \coloneqq (\pi_{\Gamma,*}\mathcal{O}_{\mathbb{H}^*})^\Gamma.$$

Theorem 2.15. *The ringed space $(X(\Gamma), \mathcal{O}_{X(\Gamma)})$ is a Riemann surface.*

Proof. We have to prove that the ringed space $(X(\Gamma), \mathcal{O}_{X(\Gamma)})$ is locally isomorphic to $\mathbb{C}$. Let $x \in X(\Gamma)$. Assume that x is nor elliptic nor a cusp and let $\tau \in \pi_\Gamma^{-1}(x)$. Then π_Γ is an isomorphism from some open neighbourhood U of τ on some open neighbourhood of x inducing an isomorphism from $(V, \mathcal{O}_{X(\Gamma)} \mid_V)$ onto $(U, \mathcal{O}_{\mathbb{H}} \mid_U)$ proving the claim at a neighbourhood of x.

Assume now that x is elliptic, let $\tau \in \pi_\Gamma^{-1}(x)$ and let U be some open neighbourhood of τ in $\mathbb{H}$ such that $\gamma(U) \cap U \neq \emptyset \Rightarrow \gamma \in \Gamma_\tau$. Then Γ_τ is a finite cyclic group. We can assume that U is stable under Γ_τ so that π_Γ induces an isomorphism $\Gamma_\tau \backslash U \xrightarrow{\sim} \pi_\Gamma(U)$. Let $\lambda : \mathbb{H} \simeq D$ be a biholomorphic map sending τ to 0. Let γ be a generator of $\overline{\Gamma}_\tau$. Then $\lambda \circ \gamma \circ \lambda^{-1}$ is an holomorphic automorphism of D fixing 0. From Schwarz Lemma, it is of the form $z \mapsto az$ for some $a \in \mathbb{C}^\times$. This implies that a is a primitive n-th root of unity where n is the cardinal of $\overline{\Gamma}_\tau$. Let U' be the image of $\lambda(U)$ under $z \mapsto z^n$. We have the following commutative diagram

$$\begin{array}{ccc} U & \xrightarrow{\lambda} & \lambda(U) \\ \downarrow{\scriptstyle \pi_\Gamma} & & \downarrow{\scriptstyle z \mapsto z^n} \\ \pi_\Gamma(U) & \xrightarrow{\simeq} & U'. \end{array}$$

An holomorphic function f on $\lambda(U)$ is invariant under $z \mapsto az$ if and only if it is of the form $z \mapsto g(z^n)$ for some holomorphic function g on U'. This remark implies that the bottom homeomorphism identifies $\pi_{\Gamma,*}\mathcal{O}_{\mathbb{H}}^{\Gamma_\tau}$ with the sheaf $\mathcal{O}_{U'}$ and proves that $X(\Gamma)$ is a Riemann surface on a neighbourhood of τ.

Finally assume that x is a cusp, that is $x = \pi_\Gamma(c)$ for some cusp c of Γ. Replacing Γ by some conjugate subgroup of $\mathrm{SL}_2(\mathbb{R})$, we can assume that $c = \infty$. We know that there exists $r > 0$ such that $\pi_\Gamma(U_{\infty,r}) \simeq \Gamma_\infty \backslash U_{\infty,r}$. Moreover there exists $h > 0$ such that $\overline{\Gamma_\infty} = \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)^{\mathbb{Z}}$. The map q_h defined on $U_{\infty,r} \smallsetminus \{\infty\}$ by $z \mapsto e^{2\pi \mathrm{i} z/h}$ is an holomorphic covering of group $\Gamma_\infty/(\Gamma_\infty \cap \{\pm I_2\})$ inducing an isomorphism of Riemann surfaces from $\Gamma_\infty \backslash (U_{\infty,r} \smallsetminus \{\infty\})$ to $D_{e^{-2\pi r/h}} \smallsetminus \{0\}$ where D_s is the open disk of radius s. Let f be an holomorphic function on $U_{\infty,r} \smallsetminus \{\infty\}$ which is invariant under Γ_∞. It is the inverse image of an holomorphic function $\tilde{f}$ on $D_{e^{-2\pi r/h}}$. The function f extends continuously to ∞ if and only if $\tilde{f}$ extends continuously to 0 and the unique continuous extension of f to $U_{\infty,r}$ is the inverse image of the unique extension of $\tilde{f}$ to the disk. A continuous function on the disk D_s which is holomorphic on $D_s \smallsetminus \{0\}$ is actually holomorphic on D_s. This implies that ringed space $(U_{\infty,r}, \mathcal{O}_{U_{\infty,r}}^{\Gamma_\infty})$ is isomorphic to the ringed space of holomorphic functions on $D_{e^{-2\pi r/h}}$. This achieves the proof. □

2.7 Arithmetic subgroups and congruence subgroups

We recall that an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$ is a discrete subgroup which is commensurable with $\mathrm{SL}_2(\mathbb{Z})$.

Let $N \geqslant 1$ and let $\Gamma(N) \coloneqq \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$. It is subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with finite index. We define a *congruence subgroup* as a discrete subgroup $\Gamma(\mathrm{SL}_2(\mathbb{Z}))$ containing $\Gamma(N)$ for some $N \geqslant 1$. A congruence subgroup is commensurable with $\mathrm{SL}_2(\mathbb{Z})$ and is consequently an arithmetic subgroup.

Remark 2.16. In $\mathrm{SL}_2(\mathbb{R})$, there exist arithmetic subgroups which are not congruence subgroups.

Let $\mathcal{D} = \{z \in \mathbb{H} \mid |\mathrm{Re}\, z| \leqslant 1,\ \ |z| \geqslant 1\}$.

Lemma 2.17. *Let $\Gamma' \subset \Gamma$ be discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$ such that $[\Gamma : \Gamma'] < +\infty$. Then $X(\Gamma)$ is compact if and only if $X(\Gamma')$ is compact.*

Proof. The quotient map $X(\Gamma') \to X(\Gamma)$ is continuous surjective so one direction is clear. It remains to prove that $X(\Gamma)$ compact implies $X(\Gamma')$ compact. Assume first that Γ' is an invariant subgroup of Γ. Then $X(\Gamma)$ is the quotient of $X(\Gamma')$ under the finite group $G = \Gamma/\Gamma'$. We know that $X(\Gamma')$ is locally compact. Let $(U_i)_{i\in I}$ be an open covering of $X(\Gamma')$ such that $\overline{U_i}$ is compact for all $i \in I$. The quotient map $\mathbb{H}^* \to X(\Gamma)$ is open. This implies that the transition map $\pi : X(\Gamma') \to X(\Gamma)$ is open. As it is surjective, the family $(\pi(U_i))_{i\in I}$ is an open covering of $X(\Gamma)$. By compactness of $X(\Gamma)$, there exists a finite subset $J \subset I$ such that $X(\Gamma) = \bigcup_{i\in J} \pi(U_i)$. Let $A = \bigcup_{i\in J} \overline{U_i}$. It is a compact subset of $X(\Gamma')$ and $X(\Gamma') = \bigcup_{g\in G} g(A)$, this proves that $X(\Gamma')$ is compact. In the general case, let $\Gamma' = \bigcup_{\gamma\in\Gamma} \gamma\Gamma'\gamma^{-1}$. It is an invariant subgroup of Γ which is of finite index in Γ. Consequently $X(\Gamma'')$ is compact and the map $X(\Gamma'') \to X(\Gamma')$ is continuous and surjective, proving that $X(\Gamma')$ is compact. □

Corollary 2.18. *If Γ is an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$, then $\Gamma\backslash\mathbb{H}^*$ is compact.*

Proof. By Lemma 2.17, it is sufficient to prove that $X(\mathrm{SL}_2(\mathbb{Z}))$ is compact. It follows from Theorem 1.10 that $X(\mathrm{SL}_2(\mathbb{Z})) = \pi_{\mathrm{SL}_2(\mathbb{Z})}(\mathcal{D})$. Consequently it is sufficient to prove that $\mathcal{D}$ is compact. This can be proved exactly as in the proof of Theorem 2.13. □

2.8 General results for Riemann surfaces

Let $f : X \to Y$ be a morphism between Riemann surfaces and let $P \in X$. Then There exists local charts (U, z) and (V, t) such that $P \in U$, $z(P) = 0$, $Q \coloneqq f(P) \in V$ and $t(Q) = 0$ and an integer $e_P \in \mathbb{N}$ such that $f \circ z^{-1} = t^{e_P(f)}$ on $z(U)$. The integer $e_P(f)$ does not depend on the choice of (U, z) and (V, t). It is called the *ramification index* of f at P. If f is not constant, the set $\{P \in X \mid e_P(f) > 1\}$ is closed and discrete in X.

Theorem 2.19. *Let $f : X \to Y$ be an holomorphic map between Riemann surfaces. Assume that X is compact. Then f is constant or surjective. If f is surjective, the quantity*

$$\sum_{\substack{P\in X\\ f(P)=Q}} e_P$$

does not depend on Q. It is called the degree *of f and noted* $\deg f$.

If f is constant, we set $\deg f = 0$. We have the property $\deg(g \circ f) = (\deg g)(\deg f)$ which is easy to check. The *genus* of a compact Riemann surface is the dimension of the finite dimensional $\mathbb{C}$-vector space $g(X) \coloneqq \dim_{\mathbb{C}} H^0(X, \Omega^1_X)$.

Theorem 2.20 (Riemann-Hurwitz)**.** *Let X and Y be two compact Riemann surfaces and let $f : X \to Y$ be a non constant holomorphic map. Then we have the formula*

$$2(g(X) - 1) = 2(g(Y) - 1) \deg f + \sum_{P \in X} (e_P(f) - 1).$$

Let X be a compact Riemann surface. A *divisor* of X is an element of the free abelian group $\mathrm{Div}(X) \coloneqq \bigoplus_{x \in X} \mathbb{Z}[x]$. There is a structure of ordered abelian group of $\mathrm{Div}(X)$ defined by

$$\sum_{x \in X} m_x[x] \geqslant 0 \Leftrightarrow \forall x \in X,\, m_x \geqslant 0.$$

If f is a non zero meromorphic function on X, f has finitely many poles and zeros and its divisor is the element

$$\mathrm{div}(f) \coloneqq \sum_{x \in X} \mathrm{ord}_x(f)[x].$$

The function div defines a group homomorphism from $\mathbb{C}(X)^\times$ to $\mathrm{Div}(X)$ whose kernel is the subgroup of non zero constant functions on X. A divisor which in the image of div is called a *principal divisor*. The subgroup of principal divisors is noted $\mathrm{Pr}(X)$. The degree map is the group homomorphism $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ such that $\deg([x]) = 1$ for all $x \in X$. Let $\mathrm{Div}^0(X)$ be the subgroup of divisors of degree 0, we have $\mathrm{Pr}(X) \subset \mathrm{Div}^0(X)$. It follows from the residue formula that $\deg \circ \mathrm{div} = 0$. Consequently we can define the quotients $\mathrm{Pic}(X) \coloneqq \mathrm{Div}(X)/\mathrm{Pr}(X)$ and $\mathrm{Pic}^0(X) \coloneqq \mathrm{Div}^0(X)$ and we have an exact sequence of abelian groups

$$0 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \xrightarrow{\deg} \mathbb{Z} \to 0.$$

If $D = \sum_{x \in X} m_x[x]$ is a divisor, we define $L(D)$ as the $\mathbb{C}$-vector subspace of $\mathbb{C}(X)$ defined by

$$L(D) = \{f \in \mathbb{C}(X) \mid D + \mathrm{div}(f) \geqslant 0\} = \{f \in \mathbb{C}(X) \mid \forall x \in X,\, \mathrm{ord}_x(f) \geqslant -m_x\}.$$

The $\mathbb{C}$ vector space is finite dimensional and we define $\ell(D) \coloneqq \dim_{\mathbb{C}} L(D)$. It is easy to check that if $L(D) \neq 0$, then $\deg D \geqslant 0$.

More generally let $\mathcal{L}$ be a line bundle on X and let s be a non zero meromorphic section of $\mathcal{L}$. For $x \in X$, the local ring $\mathcal{O}_{X,x}$ is a discrete valuation ring and $\mathcal{L}_x$ is a finite free $\mathcal{O}_{X,x}$-module of rank 1. Let $t_x \in \mathcal{O}_{X,x}$ be an uniformizer at x. We define $\mathrm{ord}_x(s) \coloneqq \min\{n \in \mathbb{Z} \mid t_x^{-n} s_x \in \mathcal{L}_x\}$. This integer is well defined, does not depend on

the choice of t_x. Moreover if $\mathcal{L} = \mathcal{O}_X$, it coincides with the usual order of s at x. The *divisor* of s is

$$\operatorname{div}(s) \coloneqq \sum_{x \in X} \operatorname{ord}_x(s)[x].$$

The image $[\operatorname{div}(s)]$ of $\operatorname{div}(s)$ in $\operatorname{Pic}(X)$ does not depend on the choice of the section s and is noted $[\mathcal{L}]$. Consequently the degree $\deg(\operatorname{div}(s))$ depends only on $\mathcal{L}$ and is called the *degree* $\deg \mathcal{L}$ of the line bundle $\mathcal{L}$. Actually the map $\mathcal{L} \mapsto [\mathcal{L}]$ induces an isomorphism between the group of isomorphism classes of line bundles on X and $\operatorname{Pic}(X)$. The class of the line bundle Ω_x is noted K_X and is called the *canonical class* of the Riemann surface X.

Theorem 2.21 (Riemann-Roch)**.** *Let X be a compact Riemann surface and let D be a divisor of X. We have*

$$\ell(D) - \ell(K_X - D) = 1 - g(X) + \deg(D).$$

Corollary 2.22. *We have $\deg K_X = 2g(X) - 2$ and, if $\deg D > 2g(X) - 2$, we have*

$$\ell(D) = 1 - g(X) + \deg(D).$$

2.9 The genus of arithmetic quotients

If $\Gamma' \subset \Gamma$ are two arithmetic subgroups, the projection $\mathbb{H}^* \to X(\Gamma)$ factors through a surjective morphism between compact Riemann surfaces

$$\pi : X(\Gamma') \to X(\Gamma).$$

This morphism is a finite morphisme between Riemann surfaces and its degree is equal to

$$[\overline{\Gamma} : \overline{\Gamma'}] = [\Gamma\{\pm I_2\} : \Gamma'\{\pm I_2\}].$$

Consequently, for each $Q \in X(\Gamma)$, we have

$$\sum_{P \in \pi^{-1}(Q)} e_P(\pi) = \deg \pi = \begin{cases} \frac{1}{2}[\Gamma : \Gamma'] & \text{if } -I_2 \in \Gamma \smallsetminus \Gamma' \\ [\Gamma : \Gamma'] & \text{in the other cases.} \end{cases}$$

Example 2.23. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Then we have $X(\Gamma) = Y(\Gamma) \coprod \{\Gamma\infty\}$. The stabilizer of the cusp ∞ is

$$\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},\ n \in \mathbb{Z} \right\}.$$

This implies that $z \mapsto q(z) = e^{2\pi i z}$ is a local parameter at $\Gamma\infty \in X(\Gamma)$. We defined a holomorphic Γ-invariant function

$$j : \mathbb{H} \to \mathbb{C} \subset \mathbb{P}^1(\mathbb{C})$$

by $z \mapsto (j(z) : 1)$. This function defines consequently a holomorphic map

$$j : Y(\mathrm{SL}_2(\mathbb{Z})) \to \mathbb{C}.$$

It follows from formula (2) that j can be extended into an holomorphic map

$$j : X(\mathrm{SL}_2(\mathbb{Z})) \to \mathbb{P}^1(\mathbb{C})$$

such that $j(\Gamma\infty) = (1, 0)$. As j is non constant, it is a surjection. Moreover this function is a local isomorphism at $\Gamma\infty$. As $\Gamma\infty$ is the only point in the preimage of $(1, 0)$ showing that it is has degree 1 and consequently is an isomorphism of Riemann surfaces. As a consequence we proved that the function $j : \mathbb{H} \to \mathbb{C}$ is surjective and that $j(z) = j(z')$ if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $z' = \gamma(z)$.

This example shows that the Riemann surface $X(\mathrm{SL}_2(\mathbb{Z}))$ is algebraic. It is actually a general fact.

From now we will sometime use the notation $g(\Gamma) \coloneqq g(X(\Gamma))$ if Γ is an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Example 2.23 implies that $g(\mathrm{SL}_2(\mathbb{Z})) = 0$. If we want to compute the genus of $X(\Gamma)$ for an arithmetic group Γ using Riemann-Hurwitz formula, we need to compute the ramification indices of the morphism $X(\Gamma) \to X(\mathrm{SL}_2(\mathbb{Z}))$.

Let $P \in \mathbb{H}$. Then the map $\pi_\Gamma : \mathbb{H} \to Y(\Gamma)$ is ramified at P (ie has a ramification index $e_P > 1$) if and only if P is an elliptic point of Γ. In this case the ramification index is exactly the order of the point P. When Γ is an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{Z})$ this order is a divisor of 3 or 2 hence can be equal to 3 or 2. Assume that $P \in \mathbb{H}$ is an elliptic point of order $i \in \{2, 3\}$ for $\mathrm{SL}_2(\mathbb{Z})$. Then the map $\pi_{\mathrm{SL}_2(\mathbb{Z})} : \mathbb{H} \to Y(\mathrm{SL}_2(\mathbb{Z}))$ is ramified of index i at P and the map $\pi_\Gamma : \mathbb{H} \to Y(\Gamma)$ is ramified (automatically of index i) at P if and only if P is an elliptic point of Γ. The factorisation

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{\pi_\Gamma} & Y(\Gamma) \\ & {\scriptstyle \pi_{\mathrm{SL}_2(\mathbb{Z})}} \searrow \quad \swarrow {\scriptstyle \pi} & \\ & Y(\mathrm{SL}_2(\mathbb{Z})) & \end{array}$$

shows that π is ramified at $\pi_\Gamma(P)$ if and only if P is *not* an elliptic point for Γ. Namely we have the factorisation of ramification indexes

$$e_P(\pi_{\mathrm{SL}_2(\mathbb{Z})}) = e_P(\pi_\Gamma) e_{\pi_\Gamma(P)}(\pi).$$

Using example 2.23, we deduce the following formula for the genus of an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 2.24. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be an arithmetic subgroup. If $i \in \{2, 3\}$, let $\nu_i(\Gamma)$ be the number of elliptic points of $Y(\Gamma)$ of order i for Γ and let $\nu_\infty(\Gamma)$ be the number of cusps of $X(\Gamma)$. Then we have the formula computing the genus of $X(\Gamma)$:*

$$g(X(\Gamma)) = 1 + \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma\{\pm I_2\}]}{12} - \frac{\nu_2(\Gamma)}{4} - \frac{\nu_3(\Gamma)}{3} - \frac{\nu_\infty(\Gamma)}{2}.$$

Proof. Let $\pi : X(\Gamma) \to X(\mathrm{SL}_2(\mathbb{Z}))$ be the projection. It is a finite map between compact Riemann surfaces of degree $\deg \pi = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma\{\pm I_2\}]$. Let $i \in \{2, 3\}$ and let $P \in \pi^{-1}(x_i)$ where $x_i \in X(\mathrm{SL}_2(\mathbb{Z}))$ is the unique elliptic point of $X(\mathrm{SL}_2(\mathbb{Z}))$ of order i. If P is an elliptic point of $X(\Gamma)$, then $e_P(\pi) = 1$ and if P is not an elliptic point then $e_P(\pi) = i$. Let $\nu_i'(\Gamma)$ be the number of points of $\pi^{-1}(x_i)$ which are not elliptic. We have consequently $\deg \pi = \nu_i(\Gamma) + i\nu_i'(\Gamma)$. Applying Riemann-Hurwitz formula (Theorem 2.20), we obtain

$$2(g(\Gamma) - 1) = 2\deg(\pi)(g(\mathrm{SL}_2(\mathbb{Z})) - 1) + \nu_2'(\Gamma) + 2\nu_3'(\Gamma) + \sum_{P \in \pi^{-1}(\infty)} (e_P(\pi) - 1).$$

Moreover we know that $\sum_{P \in \pi^{-1}(\infty)} e_P(\pi) = \deg \pi$ and $g(\mathrm{SL}_2(\mathbb{Z})) = 0$ so that

$$2(g(\Gamma) - 1) = -2\deg(\pi) + \frac{\deg \pi - \nu_2(\Gamma)}{2} + 2\frac{\deg \pi - \nu_3(\Gamma)}{3} + \deg \pi - \nu_\infty(\Gamma)$$

which gives the formula. □

Example 2.25. We consider the case of the principal congruence subgroup $\Gamma(N)$. If $N \geqslant 2$ is has no elliptic point. Namely, it is normal in $\mathrm{SL}_2(\mathbb{Z})$, hence if it has an elliptic point of order 2, it has to contain an elliptic element stabilizing i, namely $\pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. And none of these matrices is in $\Gamma(N)$ for $N \geqslant 2$. An analogous reasoning shows that it does not have order three elliptic points. The degree $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ can be easily calculated, it is $\operatorname{Card} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is $N = 2$ and $\frac{1}{2} \operatorname{Card} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ if $N \geqslant 3$. Consequently

$$\mu_N \coloneqq \deg \pi_{\mathrm{SL}_2(\mathbb{Z})/\Gamma(N)} = \begin{cases} \frac{N^3}{2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right) & \text{if } N \geqslant 3 \\ 6 & \text{if } N = 2. \end{cases}$$

Finally $\Gamma(N)$ being normal in $\mathrm{SL}_2(\mathbb{Z})$, the group $\mathrm{SL}_2(\mathbb{Z})$ acts on $X(\Gamma(N))$ and acts transitively on the cusps of $X(\Gamma(N))$. Consequently it is sufficient to compute the ramification index of $\pi_{\mathrm{SL}_2(\mathbb{Z})/\Gamma(N)}$ at one cusps. Do it at ∞. We have

$$\Gamma(N)_\infty = \begin{cases} \left\{ \begin{pmatrix} 1 & Nk \\ 0 & 1 \end{pmatrix}, k \in \mathbb{Z} \right\} & \text{if } N \geqslant 3 \\ \left\{ \pm \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}, k \in \mathbb{Z} \right\} & \text{if } N = 2. \end{cases}$$

Consequently the ramification index at cusps is equal to N and we have

$$\nu_\infty(\Gamma(N)) = \frac{\mu_N}{N}.$$

We can conclude that

$$g(\Gamma(N)) = 1 + \frac{\mu_N}{12N}(N - 6).$$

There are other congruences subgroups that we can consider. For $N \geqslant 1$, we define

$$\Gamma_0(N) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid N|c \right\}, \quad \Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \equiv 1\,[N] \right\}.$$

Note that $\Gamma_0(N)$ and $\Gamma_1(N)$ are congruence subgroups since

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}).$$

We easily check that we have $\Gamma_0(2) = \Gamma_1(2)$ and

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)\{\pm I_2\}] = \begin{cases} \frac{N^2}{2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right) & \text{if } N \geqslant 3 \\ 3 & \text{if } N = 2. \end{cases}$$

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

Proposition 2.26. *If $N \geqslant 4$, the group $\Gamma_1(N)$ has no elliptic element. We have $\nu_2(\Gamma_1(2)) = \nu_3(\Gamma_1(3)) = 1$ and $\nu_2(\Gamma_1(3)) = \nu_3(\Gamma_1(2)) = 0$.*

Proof. We have $\operatorname{Tr}\gamma \equiv 2\,[N]$ for $\gamma \in \Gamma_1(N)$. Consequently if $\nu_2(\Gamma_1(N)) \neq 0$, we must have $N \mid 2$, ie. $N = 2$. If $\nu_3(\Gamma_1(N)) \neq 0$, we must have $N = 3$ and $\operatorname{Tr}\gamma = -1$ if $\gamma \in \Gamma_1(N)$ is elliptic. The equalities $\nu_2(\Gamma_1(2)) = \nu_3(\Gamma_1(3)) = 1$ are an exercice for the reader. □

Lemma 2.27. *Let $N \geqslant 1$. Then the morphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_Z(\mathbb{Z}/N\mathbb{Z})$ given by reduction modulo N is surjective.*

Proof. It is sufficient to check that the two matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ generate $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. □

Lemma 2.28. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup containing $\Gamma(N)$. Let Γ_N be the image of Γ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $U_N \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the subset of elements of order exactly N in $(\mathbb{Z}/N\mathbb{Z})^2$. Then there exists a bijection of finite sets*

$$\Gamma \backslash \mathbb{P}^1(\mathbb{Q}) \simeq \Gamma_N \backslash U_N / \{\pm I_2\}.$$

Proof. Let $P \subset \mathrm{SL}_2(\mathbb{Z})$ be the subgroup of upper triangular matrices. The group P is the stabilizer of $(A : 0)$ in $\mathbb{P}^1(\mathbb{Q})$ and the group $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$. Consequently $\mathbb{P}^1(\mathbb{Q}) \simeq \mathrm{SL}_2(\mathbb{Z})/P$ and this bijection is compatible to the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Q})$ and on $\mathrm{SL}_2(\mathbb{Z})/P$ on the left. Since $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$, we have

$$\Gamma \backslash \mathbb{P}^1(\mathbb{Q}) \simeq \Gamma \backslash \mathrm{SL}_2(\mathbb{Z}) / \Gamma(N) P \simeq \Gamma_N \backslash \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) / P_N.$$

The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is acting transitively on U_N and the stabilizer of the vector $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ is the subgroup of matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. This proves the assertion. □

Corollary 2.29. *If $c \in \mathbb{P}^1(\mathbb{Q})$, there exists coprime elements a and b in $\mathbb{Z}$ such that $c = (a : b)$. The vector $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ is well defined up to a sign, so that there is a well defined map*

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{Q}) & \longrightarrow & U_N/\{\pm I_2\} \\ (a:b) & \longmapsto & \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]. \end{array}$$

This map induces a bijection from the set of cusps of the group $\Gamma(N)$ to the finite set $U_N/\{\pm I_2\}$.

Proposition 2.30. *For $N \geqslant 2$, we have*

$$\nu_\infty(\Gamma_1(N)) = \begin{cases} \frac{1}{2}\sum_{\substack{d \geqslant 1 \\ d|N}} \varphi(d)\varphi(N/d) & \text{if } N \geqslant 5 \text{ or } N = 3 \\ 3 & \text{for } N = 4 \\ 2 & \text{for } N = 2 \end{cases}$$

$$\nu_\infty(\Gamma_0(N)) = \sum_{\substack{d \geqslant 1 \\ d|N}} \varphi(d \wedge N/d).$$

Proof. Two elements $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a' \\ b' \end{smallmatrix}\right]$ of U_N are in the same orbit of $\Gamma_1(N)$ if and only if there exists $n \in \mathbb{Z}$ such that $b' = b$ and $a' = (a + nb)$ in $\mathbb{Z}/N\mathbb{Z}$. Assume that b as order $d \mid N$ in $\mathbb{Z}/N\mathbb{Z}$, then there are exactly $\varphi(N/d)$ classes of $a \in \mathbb{Z}$ for the equivalence relation $a \sim a' \Leftrightarrow a' \in a + b\mathbb{Z}$ such that $a \wedge N = 1$. There is $\varphi(d)$ elements of order d in $\mathbb{Z}/N\mathbb{Z}$ so that

$$\mathrm{Card}\,(\Gamma_1(N)\backslash U_N) = \sum_{\substack{d \geqslant 1 \\ d|N}} \varphi(d)\varphi(N/d).$$

To obtain the formula, we have to prove that the group $\{\pm I_2\}$ has no fixed point on $\Gamma_1(N)\backslash\, U_N$ for $N \geqslant 5$ or $N = 3$. If the class $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ is a fixed point, then $2b = 0$ in $\mathbb{Z}/N\mathbb{Z}$ so that $b = 0$ or N is even and $b = N/2$. If $b = 0$, we have $2a = 0$ in $\mathbb{Z}/N\mathbb{Z}$ which contradicts $a \wedge b = 1$. If $b = N/2$ then, $2a = 0$ in $\mathbb{Z}/(N/2)\mathbb{Z}$. Assume $N > 2$, then $a \neq 0$ in $\mathbb{Z}/N\mathbb{Z}$ and we must have $4 \mid N$ and $a \in \mathbb{Z}(N/4)$. The condtion $a \wedge b = 1$ implies $N = 4$. A direct inspection shows that $\Gamma_1(2)\backslash U_2/\{\pm I_2\} = \Gamma_1(2)\backslash U_2$ has two elements represented by $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ while $\Gamma_1(4)\backslash U_4/\{\pm I_2\}$ has three elements represented by $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right]$. We can remark that the class of $\left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right]$ in $\Gamma_1(4)\backslash U_4$ is fixed by $\{\pm I_2\}$.

First of all we can remark that $\{\pm I_2\}$ is contained in $\Gamma_0(N)$ so that $\nu_\infty(\Gamma_0(N))$ is the number of orbits of $\Gamma_0(N)$ on U_N. Two elements $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a' \\ b' \end{smallmatrix}\right]$ of U_N represent the same cusp of $\Gamma_0(N)$ if and only if there exists $n \in \mathbb{Z}$ and $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $b' = \alpha^{-1}b$ and $a' = \alpha a + nb$. The orbits of $(\mathbb{Z}/N\mathbb{Z})^\times$ acting on $\mathbb{Z}/N\mathbb{Z}$ are parametrized by positive divisors of N. Consequently for each orbit of $\Gamma_0(N)$ on U_N there is a well defined positive divisor d of N such that an element of the form $\left[\begin{smallmatrix} a \\ d \end{smallmatrix}\right]$ is in the orbit. Two elements $\left[\begin{smallmatrix} a \\ d \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a' \\ d \end{smallmatrix}\right]$ are in the same orbit if and only if there exists $\alpha \in 1 + (N/d)\mathbb{Z}$

such that $a' = \alpha a$ in $(\mathbb{Z}/d\mathbb{Z})^\times$. This proves that there exists exactly

$$\sum_{\substack{d \geqslant 1 \\ d|N}} \varphi(d \wedge (N/d))$$

orbits for the action of $\Gamma_0(N)$ on U_N. □

Example 2.31. The group $\Gamma_1(5)$ has 4 cusps which are represented by the elements

$$\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 \\ 2 \end{smallmatrix}\right].$$

Corollary 2.32. *We have, for $N > 1$,*

$$g(\Gamma_1(N)) = \begin{cases} 1 + \frac{N^2}{24} \prod_{p|N} \left(1 - \frac{1}{p^2}\right) - \frac{1}{4} \sum_{\substack{d \geqslant 1 \\ d|N}} \varphi(d)\varphi(N/d) & \text{if } N \geqslant 5; \\ 0 & \text{if } N \in \{2, 3, 4\}. \end{cases}$$

Remark 2.33. Actually, $g(\Gamma_1(N)) = 0$ if $N \leqslant 10$ or $N = 12$. We have $g(\Gamma_1(11)) = 1$, $g(\Gamma_1(13)) = 2$, $g(\Gamma_1(14)) = 1 \ldots$

Exercice 2.1. Prove that $g(\Gamma_1(N)) = 0 \Leftrightarrow N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.

The congruence subgroups of the form $\Gamma_0(N)$ can have a lot of elliptic points. They are counted by the following result.

Theorem 2.34. *We have, for $N \geqslant 3$,*

$$\nu_2(\Gamma_0(N)) = \begin{cases} 0 & \text{if } 4 \mid N \\ \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{in other cases} \end{cases}$$

$$\nu_3(\Gamma_0(N)) = \begin{cases} 0 & \text{if } 9 \mid N \\ \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{in other cases} \end{cases}.$$

Example 2.35. If p is a prime, the map $X(\Gamma_0(p)) \to X(\mathrm{SL}_2(\mathbb{Z})) \simeq \mathbb{P}^1(\mathbb{C})$ has degree $p + 1$. The curve $X(\Gamma_0(p))$ has two cusps which are the equivalence classes of ∞ and 0. The map is unramified at ∞ but has ramification index p at 0. Moreover we have

$$g(X(\Gamma_0(p))) = \begin{cases} \frac{p-13}{12} & \text{if } p \equiv 1\,[1]2 \\ \frac{p-5}{12} & \text{if } p \equiv 5\,[1]2 \\ \frac{p-7}{12} & \text{if } p \equiv 7\,[1]2 \\ \frac{p+1}{12} & \text{if } p \equiv -1\,[1]2 \\ 0 & \text{if } p \in \{2, 3\}. \end{cases}$$

The curves $X_0(p)$ for $p \in \{2, 3, 5, 7, 13\}$ are isomorphic to $\mathbb{P}^1(\mathbb{C})$. The curves $X_0(p)$ for $p \in \{11, 17, 19\}$ are elliptic curves and, for $p \geqslant 23$, they have genus $\geqslant 2$.

3 Modular forms

3.1 Definitions

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be an arithmetic subgroup and let $k \in \mathbb{Z}$.

Definition 3.1. *A function $f : \mathbb{H} \to \mathbb{C}$ is* weakly modular of weight k and level Γ *if it is meromorphic and if*

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. For $z \in \mathbb{H}$, we define $j(g,z) \coloneqq (cz+d)$. We have $j(gh,z) = j(g,h(z))j(h,z)$. This proves that if we define

$$(f \mid_k g)(z) \coloneqq j(g,z)^{-k} f(g(z)),$$

the map $(g,f) \mapsto (f \mid_k g)$ defines a right action of $\mathrm{SL}_2(\mathbb{R})$ on the space of holomorphic functions on $\mathbb{H}$. The space of weakly modular functions of weight k and level Γ is the subspace of Γ-invariant functions for this action.

Let f be a weakly modular function of weight k and level Γ. Assume that ∞ is a cusp of Γ. There exists $h > 0$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_\infty$. The map $z \mapsto q_h(z) = e^{\frac{2\pi i}{h} z}$ is an holomorphic covering $\mathbb{H} \to D^*$. Then $f(z+h) = f(z)$ and there exists a meromorphic function $\tilde{f}$ defined on D^* such that $f = \tilde{f} \circ q_h$. We say that f is *meromorphic at* ∞ (resp. *holomorphic at* ∞, resp. *cuspidal at* ∞) if $\tilde{f}$ is meromorphic (resp. holomorphic, resp. holomorphic and vanishing at 0) on D. The following Lemma shows that this definition does not depend on the choice of the real number $h > 0$.

Lemma 3.2. *Let f be an holomorphic function on D^* and let $n \in \mathbb{N}^*$. Then f is meromorphic (resp. holomorphic) on D if and only if $z \mapsto f(z^n)$ is meromorphic (resp. holomorphic) on D.*

Proof. The function f is meromorphic on D if and only if there exists an integer $m \geqslant 0$ such that $z \mapsto z^m f(z)$ is holomorphic on D. Consequently it is sufficient to consider the case of holomorphic function. However an holomorphic function on D^* is holomorphic on D if and only if it has a limit in 0 and f has a limit in 0 if and only if $z \mapsto f(z^n)$ has. □

Let c be a cusp of Γ, there exists $\sigma \in \mathrm{SL}_2(\mathbb{R})$ such that $c = \sigma(\infty)$. So that ∞ is a cusp of $\sigma^{-1}\Gamma\sigma$. A function f is weakly modular of weight k and level Γ if and only if $f \mid_k \sigma$ is weakly modular of weight k and level $\sigma^{-1}\Gamma\sigma$. We say that f is *meromophic at* c (resp. *holomorphic at* c, resp. *cuspidal at* c) if $f \mid_k \sigma$ is meromophic at ∞ (resp. holomorphic at ∞, resp. cuspidal at ∞). This definition does not depend on the choice of σ such that $c = \sigma(\infty)$.

Definition 3.3. *A* modular form of weight k and level Γ *is a weakly modular function of weight k and level Γ which is holomorphic on $\mathbb{H}$ and holomorphic at all the cusps of Γ. We say that a modular form f is* cuspidal *if it is cuspidal at all the cusps of Γ. A* meromorphic modular form of weight k and level Γ *is a weakly modular function of weight k and level Γ which is meromorphic at all the cusps of Γ.*

We note $M_k(\Gamma)$ the $\mathbb{C}$-vector space of modular forms of weight k and level Γ and $S_k(\Gamma)$ its subspace of cuspidal forms.

A very useful notion related to modular curves is the notion of Fourier series or q-development. Let f be a weakly modular form of weight k and level Γ and let c be a cusp of Γ and let $\sigma \in \mathrm{SL}_2(\mathbb{R})$ such that $c = \sigma(\infty)$. Assume in a first time that the cusp is *regular* which means that there exists a real $h > 0$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \sigma^{-1}\Gamma_c\sigma$ and generates $\sigma^{-1}\overline{\Gamma_c}\sigma$. The function $\tilde{f}_c$ on $D^\times$ such that $f \mid \sigma = \tilde{f}_c \circ q_h$ is meromorphic with at most one pole at 0 which means that it can be written as a Laurent series

$$\tilde{f}_c(q_h) = \sum_{n=-m}^{+\infty} a_n q_h^n.$$

This Laurent series does not depend on the choice of σ and is called the *Fourier series of f at the cusp c*. If c is not regular, then we can find a generator of $\sigma^{-1}\overline{\Gamma}\sigma$ of the form $\left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right)$. If k is even, there exists a meromorphic function $\tilde{f}_c$ on D^* such that $\tilde{f}_c \circ q_h = f \mid_k \sigma$ which is called the Fourier series of f at c. However if k is odd, we have $f(z+h) = -f(z)$ and we define the Fourier series of f at c as being the unique Laurent series $\tilde{f}_c$ such that $\tilde{f}_c \circ q_{2h} = f \mid_k \sigma$.

Remark 3.4. There are few classical congruence subgroups having irregular cusps. Namely if Γ has some irregular cusp, then $-I_2 \notin \Gamma$. Moreover this implies that there exists an element $\gamma = \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right)$ in Γ such that $\mathrm{Tr}\,\gamma = -2$. Consequently, for all $N \geqslant 1$, the group $\Gamma_0(N)$ has only regular cusps. As elements of the groups $\Gamma_1(N)$ and $\Gamma(N)$ are such that $\mathrm{Tr}\,\gamma \equiv 2\,[N]$, the existence of irregular cusps implies $N \mid 4$. Since $-I_2 \in \Gamma(2)$, the groups $\Gamma_1(4)$ and $\Gamma(4)$ are the only congruences subgroups among $\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$ having potentially irregular cusps. We can check that all the 6 cusps of $\Gamma(4)$ regular and that, among the three cusps of $\Gamma_1(4)$, there is only one irregular cusp, represented by $[\frac{1}{2}]$.

Exercice 3.1. Assume that $-I_2 \notin \Gamma$. Prove that a point of $\Gamma\backslash U_N$ represents an irregular cusp if and only it is fixed by $-I_2$.

When Γ is an arithmetic group having ∞ as a cusp, we will sometime abuse and speak about *the* Fourier expansion of a modular form f for the Fourier expansion at ∞.

Example 3.5. It follows from Theorem 1.8 that, for $k \geqslant 2$, the function G_{2k} is a modular form of weight $2k$ and level $\mathrm{SL}_2(\mathbb{Z})$. The function Δ is a cuspidal modular form of weight 12 and level $\mathrm{SL}_2(\mathbb{Z})$. We can remark that $G_{2k}(\infty) = 2\zeta(2k) > 0$, so that G_{2k} is not cuspidal. As the group $\mathrm{SL}_2(\mathbb{Z})$ has a unique cusp, we can conclude that for $k \geqslant 2$, we have $M_{2k}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}G_{2k} \oplus S_{2k}(\mathrm{SL}_2(\mathbb{Z}))$.

3.2 Dimension of spaces of modular forms

Let Γ be some arithmetic group. The map $\pi : \mathbb{H} \to Y(\Gamma)$ is a non constant map between two Riemann surfaces. Consequently if f is a meromorphic function on $Y(\Gamma)$, the function $\pi^*(f) \coloneqq f \circ \pi$ is weakly modular of weight 0. Conversely if g is a weakly modular function of weight 0 on $\mathbb{H}$, then there exists a unique meromorphic function f on $Y(\Gamma)$ such that $g = \pi^*(f)$.

Moreover one can check from the definition of the complex structure on $X(\Gamma)$ (and the proof of Theorem 2.15) that, for f a meromorphic function on $Y(\Gamma)$, then f is a meromorphic function on $X(\Gamma)$ if and only if $\pi^*(f)$ is a weakly modular function of weight 0 which is meromorphic at all cusps.

We remark that if ω is a differential form on $Y(\Gamma)$, then $\pi^*\omega = f\,\mathrm{d}z$ for a unique meromorphic function f on $\mathbb{H}$ and the map π^* induces an isomorphism from the complex vector space of meromorphic differentials on $Y(\Gamma)$ and the $\mathbb{C}$-vector space of weakly modular functions of weight 2 on $\mathbb{H}$. Namely, it is sufficient to check that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* \mathrm{d}z = (cz+d)^{-2}\,\mathrm{d}z.$$

Lemma 3.6. *Let ω be a meromophic differential form on $Y(\Gamma)$. Then ω is a meromorphic differential form on $X(\Gamma)$ if and only if $\pi^*\omega = f\,\mathrm{d}z$ with f a weakly modular form of weight 2 which is meromorphic at all cusps.*

Proof. We will use the local description given in the proof of Theorem 2.15. We can restrict ourselves to prove that for f a meromorphic weakly modular function of weight 2 on $\mathbb{H}$, the meromorphic differential ω on $Y(\Gamma)$ which is such that $\pi^*\omega = f\,\mathrm{d}z$ is meromorphic at the cusp $\pi(\infty)$ if and only if f is meromorphic at ∞. Let r, h and $\tilde{f}$ be as in the proof of Theorem 2.15. Let q the function $z \mapsto e^{2\pi i z/h}$ defined on $\Gamma_\infty\backslash U_{\infty,r}$ which is a local coordinate on $X(\Gamma)$ at the neighborhood of $\pi(\infty)$. Consequently it is sufficient to check that $\pi^*(\mathrm{d}q) = g(z)\,\mathrm{d}z$ for some holomorphic function on $U_{\infty,r}$ which is meromorphic in q. That is indeed the case since we have $\pi^*\,\mathrm{d}q = \frac{2\pi i}{h} q\,\mathrm{d}z$. □

This computation shows that if ω is a differential form on $X(\Gamma)$ and $\pi^*\omega = f(\tau)\,\mathrm{d}\tau$, then$\omega$ is holomorphic at a cusp c if and only if f is cuspidal at c. Consequently, we have an isomorphism of $\mathbb{C}$-vector spaces

$$H^0(X(\Gamma), \Omega^1) \simeq S_2(\Gamma)$$

showing that $\dim_{\mathbb{C}} S_2(\Gamma) = g(\Gamma)$.

Theorem 3.7. *Let $k \in \mathbb{Z}$ and let Γ be an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then the space $M_k(\Gamma)$ is finite dimensional over $\mathbb{C}$. Let g be the genus of $X(\Gamma)$, $\nu_\infty(\gamma)^{\mathrm{reg}}$ the number of regular cusps of Γ, $\nu_\infty(\Gamma)^{\mathrm{irreg}}$ the number of irregular cusps and $\nu_\infty(\Gamma) = \nu_\infty(\Gamma)^{\mathrm{reg}} + \nu_\infty(\Gamma)^{\mathrm{irreg}}$. We have*

(i) if $k < 0$, then $M_k(\Gamma) = 0$;

(ii) if k is even,

$$\dim_{\mathbb{C}} M_k(\Gamma) = (k-1)(g-1) + \sum_{x \in Y(\Gamma)} \left\lfloor \frac{k}{2}\left(1 - \frac{1}{e_x}\right)\right\rfloor + \frac{k}{2}\nu_\infty(\Gamma);$$

$$\dim_{\mathbb{C}} S_k(\Gamma) = \begin{cases} g & \text{if } k = 2 \\ (k-1)(g-1) + \sum_x \left\lfloor \frac{k}{2}\left(1 - \frac{1}{e_x}\right)\right\rfloor + \frac{k-2}{2}\nu_\infty(\Gamma); & \end{cases}$$

(iii) if $k \geqslant 3$ is odd and $-I_2 \notin \Gamma$,

$$\dim_{\mathbb{C}} M_k(\Gamma) = (k-1)(g-1) + \sum_x \left\lfloor \frac{k}{2}\left(1 - \frac{1}{e_x}\right)\right\rfloor + \frac{k}{2}\nu_\infty^{\mathrm{reg}} + \frac{k-1}{2}\nu_\infty^{\mathrm{irreg}};$$

$$\dim_{\mathbb{C}} S_k(\Gamma) = (k-1)(g-1) + \sum_x \left\lfloor \frac{k}{2}\left(1 - \frac{1}{e_x}\right)\right\rfloor + \frac{k-2}{2}\nu_\infty^{\mathrm{reg}} + \frac{k-1}{2}\nu_\infty^{\mathrm{irreg}}.$$

Proof. We will only give details in the case even case. Let $k \in \mathbb{Z}$. We already showed that the map $f \mapsto f(\tau)(\mathrm{d}\tau)^{\otimes k}$ induces a bijection from the set of weakly modular forms meromorphic at cusps of weight $2k$ and meromorphic sections of $(\Omega^1_{X(\Gamma)})^{\otimes k}$. We need to determine at which condition on the poles of $f(\tau)(\mathrm{d}\tau)^{\otimes k}$, the form g is holomorphic at a point of $\mathbb{H}$ or at a cusp.

Let $P \in \mathbb{H}$ and $Q = \pi_\Gamma(P)$. Let $\omega = f(\tau)(\mathrm{d}\tau)^{\otimes k}$ the corresponding form on $X(\Gamma)$. As $\tau - P$ is a local parameter on $\mathbb{H}$ at P, $\tau' = (\tau - P)^{e_P}$ is a local parameter at Q on $X(\Gamma)$. Writing locally $\omega = g(\tau')(\mathrm{d}\tau')^{\otimes k}$, we have

$$f(\tau)(\mathrm{d}\tau)^{\otimes k} = g((\tau - P)^{e_P}) e_P^k (\tau - P)^{k(e_P - 1)}\,\mathrm{d}\tau$$

so that

$$\operatorname{ord}_P f = e_P \operatorname{ord}_Q g + k(e_P - 1) = e_P \operatorname{ord}_Q \omega + k(e_P - 1).$$

Consequently, f is holomorphic at P if and only if

$$\operatorname{ord}_P f \geqslant 0 \Leftrightarrow \operatorname{ord}_Q \omega \geqslant -k\left(1 - \frac{1}{e_P}\right) \Leftrightarrow \operatorname{ord}_Q(g) \geqslant -\left\lfloor k\left(1 - \frac{1}{e_P}\right)\right\rfloor.$$

Now we assume that P is a cusp. We can assume that $P = \infty$. Let $Q = \pi_\Gamma(P)$. Let $h > 0$ be such that $\overline{\Gamma}_Q$ is generated by $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$. Then q_h is a local parameter of $X(\Gamma)$ at Q. Consequently we can write

$$f(\tau)(\mathrm{d}\tau)^{\otimes} = g(q_h)(\mathrm{d}q_h)^{\otimes k}$$

locally at Q. As $\mathrm{d}q_h = \frac{2\pi i}{h} q_h\,\mathrm{d}\tau$, we obtain the equality

$$\tilde{f}(q_h)\,\mathrm{d}\tau = g(q_h)\left(\frac{2\pi i}{h}\right)^k q_h^k (\mathrm{d}\tau)^{\otimes k}$$

ie $\operatorname{ord}_P f = k + \operatorname{ord}_Q \omega$. Consequently f is holomorphic at P if and only if

$$\operatorname{ord}_Q \omega \geqslant -k.$$

Consequently we define the divisor D of $X(\Gamma)$ by

$$D = \sum_{P \in Y(\Gamma)} \left\lfloor k\left(1 - \frac{1}{e_P}\right)\right\rfloor [P] + \sum_{P \in X(\Gamma) \smallsetminus Y(\Gamma)} k[P].$$

We just proved that $f \in M_{2k}(\Gamma)$ if and only if $f(\tau)(\mathrm{d}\tau)^{\otimes k}$ is a section of the line bundle

$$(\Omega^1_{X(\Gamma)})^{\otimes k} \otimes \mathcal{O}(D).$$

Consequently $M_{2k}(\Gamma)$ is finite dimensional and

$$\dim_{\mathbb{C}} M_{2k}(\Gamma) = \ell(kK + D).$$

We can compute the degree of this divisor

$$\deg(kK + D) = k(2g(\Gamma) - 2) + \sum_{P \in Y(\Gamma)} \left\lfloor k\left(1 - \frac{1}{e_P}\right)\right\rfloor + k\nu_\infty(\Gamma).$$

We see that $\deg(kK + D) < 0$ if $k < 0$, proving $M_{2k}(\Gamma) = 0$ for $k < 0$. Moreover, as Γ is an arithmetic group, we have $\nu_\infty(\Gamma) > 0$ so that $\deg(kK + D) > 2(g(\Gamma) - 2)$. We can apply Riemann-Roch Theorem and conclude that

$$\dim_{\mathbb{C}} M_{2k}(\Gamma) = 1 - g(\Gamma) + \deg(kK + D)$$

which gives the desired formula. □

Remark 3.8. 1. In the case of even k, the sum over x is actually over elliptic points of Γ since $e_x = 1$ when x is not elliptic.

2. If $-I_2 \notin \Gamma$, then Γ has no elliptic point of order 2, this is why only elliptic points of order 3 appear in the formula for odd k.

3. If $-I_2 \notin \Gamma$, it can be proved that $\nu_\infty(\Gamma)^{\mathrm{reg}}$ is indeed an even integer.

3.3 Example

If $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, we have

$$\dim_{\mathbb{C}} M_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2\,[1]2 \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2\,[1]2. \end{cases}$$

We already met the modular form $G_{2k} \in M_{2k}(\Gamma)$ for $k \geqslant 2$. Its q-expansion is

$$G_{2k}(z) = 2\zeta(2k) + 2\frac{(2\pi \mathrm{i})^{2k}}{(2k-1)!} \sum_{n \geqslant 1} \left(\sum_{\substack{d|n \\ d \geqslant 1}} d^{2k-1} \right) q^n.$$

Comme $\zeta(2k) \neq 0$, the form G_{2k} is not cuspidal and we have $M_{2k}(\Gamma) = \mathbb{C}G_{2k}$ for $k \in \{2, 3, 4, 5\}$. In general

$$M_{2k}(\Gamma) = \mathbb{C}G_{2k} \oplus S_{2k}(\Gamma).$$

Let $g_4 = 60G_4$, $g_6 = 140G_6$ and $\Delta = g_4^3 - 27g_6^2$. We already proved that $\Delta \neq 0$ and that Δ is cuspidal modular form of weight 12. More generally the two forms G_4 and G_6 generate all modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 3.9. *Recall that here* $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

(i) The multiplication by Δ *induces an isomorphism*

$$M_{k-12}(\Gamma) \xrightarrow{\sim} S_k(\Gamma).$$

(ii) Each element of $\bigoplus_{k \geqslant 0} M_{2k}(\Gamma)$ *is a polynomial in* G_4 *and* G_6 *:*

$$\bigoplus_{k \geqslant 0} M_{2k}(\Gamma) = \mathbb{C}[G_4, G_6].$$

3.4 Hecke operators

Let $\Gamma_2 \subset \Gamma_1$ be two congruence subgroups and let $f \in M_k(\Gamma_1)$ be some modular form. Then $f \in M_k(\Gamma_2)$. When Γ_2 is a normal subgroup of Γ_1, we can define an action of Γ_1 on $M_k(\Gamma_2)$ such that $M_k(\Gamma_1) = M_k(\Gamma_2)^{\Gamma_1}$. Namely if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})_+$ and f is a function on $\mathbb{H}$, we define

$$f[\gamma]_k(z) \coloneqq \det(\gamma)^{k-1}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

This defines a *right* action of the group $\mathrm{GL}_2(\mathbb{Q})_+$ on functions over $\mathbb{H}$.

Lemma 3.10. *If* Γ_2 *is a normal congruence subgroup of the congruence subgroup* Γ_1*, then* $M_k(\Gamma_2)$ *is stable under the action of* Γ_1 *and we have*

$$M_k(\Gamma_1) = M_k(\Gamma_2)^{\Gamma_1}.$$

More generally if Γ *is a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *and* $\alpha \in \mathrm{GL}_2(\mathbb{Q})_+$*, then* $\alpha^{-1}\Gamma\alpha$ *contains a congruence subgroup* Γ' *and*

$$M_k(\Gamma)[\alpha]_k \subset M_k(\Gamma').$$

Proof. Essentially an exercice. For the existence of Γ', we can remark that there exists $N \geqslant 1$ such that $\Gamma(N) \subset \Gamma$. Let M such that both $M\alpha$ and $M\alpha^{-1}$ are in $\mathcal{M}_2(\mathbb{Z})$, then we have

$$\alpha\Gamma(NM^2)\alpha^{-1} \subset \Gamma(N)$$

which implies the claim. □

We can consequently define the $\mathbb{C}$-vector spaces

$$\widetilde{M}_k = \bigcup_{\Gamma \subset \mathrm{SL}_2(\mathbb{Z})} M_k(\Gamma), \quad \widetilde{S}_k = \bigcup_{\Gamma \subset \mathrm{SL}_2(\mathbb{Z})} S_k(\Gamma)$$

where the union are on congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. The lemma implies that the group $\mathrm{GL}_2(\mathbb{Q})_+$ acts on the right on these spaces via $(\gamma, f) \mapsto f[\gamma]_k$.

Let's consider now two congruence subgroups Γ_1 and Γ_2 and some $\alpha \in \mathrm{GL}_2(\mathbb{Q})_+$. The group Γ_1 acts on the left on the double class $\Gamma_1\alpha\Gamma_2$ and there is a bijection

$$\Gamma_1\backslash\Gamma_1\alpha\Gamma_2 \simeq (\Gamma_2 \cap \alpha^{-1}\Gamma_1\alpha)\backslash\Gamma_2$$

proving that these sets are finite. We can consequently write

$$\Gamma_1\alpha\Gamma_2 = \coprod_{i=1}^{r} \Gamma_1\alpha_i.$$

If $f \in M_k(\Gamma_1)$, then the function $\sum_{i=1}^r f[\alpha_i]_k$ does not depend on the choice of the representatives α_i but only on the double class $\Gamma_1\alpha\Gamma_2$. We can consequently define

$$f[\Gamma_1\alpha\Gamma_2]_k \coloneqq \sum_{i=1}^{r} f[\alpha_i]_k.$$

The following result is easy to check :

Lemma 3.11. *If $f \in M_k(\Gamma_1)$, then $f[\Gamma_1\alpha\Gamma_2]_k \in M_k(\Gamma_2)$ and the map $f \mapsto f[\Gamma_1\alpha\Gamma_2]_k$ sends $S_k(\Gamma_1)$ into $S_k(\Gamma_2)$.*

An *Hecke operator* is an operator of the form $f \mapsto f[\Gamma_1\alpha\Gamma_2]_k$.

Composition law Consider three congruences subgroups Γ_1, Γ_2 and Γ_3. For α and β in $\mathrm{GL}_2(\mathbb{Q})_+$, the subset $\Gamma_1\alpha\Gamma_2\beta\Gamma_3$ of $\mathrm{GL}_2(\mathbb{Q})_+$ is stable by multiplication on the left by elements of Γ_1 and on the right by elements of Γ_3, it is consequently a union of double classes. More precisely, if $\Gamma_1\alpha\Gamma_2 = \coprod_{i=1}^r \Gamma_1\alpha_i$ and $\Gamma_2\beta\Gamma_3 = \coprod_{j=1}^s \Gamma_2\beta_j$, we have

$$\Gamma_1\alpha\Gamma_2\beta\Gamma_3 = \bigcup_{(i,j)} \Gamma_1\alpha_i\beta_j$$

so that $\Gamma_1\alpha\Gamma_2\beta\Gamma_3$ is a *finite* union of double classes. Let γ be such that $\Gamma_1\gamma\Gamma_3 \subset \Gamma_1\alpha\Gamma_2\beta\Gamma_3$. Then

$$\Gamma_1\gamma\Gamma_3 = \coprod_{l=1}^{t} \Gamma_1\gamma_l$$

and each $\Gamma_1\gamma_l$ is of the form $\Gamma_1\alpha_i\beta_j$ for certain pairs (i,j). The important point is that one l can correspond to several (i,j) and we define

$$m(\alpha,\beta;\gamma) = \sharp\{(i,j) \mid \Gamma_1\alpha_i\beta_j = \Gamma_1\gamma_l\}.$$

Lemma 3.12. *The quantity $m(\alpha,\beta;\gamma)$ does not depend on the choice of the α_i, β_j and γ_l, but only on the double cosets $\Gamma_1\alpha\Gamma_2$, $\Gamma_2\beta\Gamma_3$ and $\Gamma_1\gamma\Gamma_3$.*

Proof. Indeed an elementary manipulation shows that $m(\alpha,\beta;\gamma)$ is the number of Γ_2 orbits in $\Gamma_2\alpha^{-1}\Gamma_1\gamma_l \cap \Gamma_2\beta\Gamma_3$ which does not depend on the choice of γ_l. □

These multiplicity numbers determine the composition law of Hecke operators.

Proposition 3.13. *In $\mathrm{Hom}_{\mathbb{C}}(M_k(\Gamma_1), M_k(\Gamma_3))$ we have an equality*

$$[\Gamma_1\alpha\Gamma_2]_k \circ [\Gamma_2\beta\Gamma_3]_k = \sum_{\Gamma_1\gamma\Gamma_3 \subset \Gamma_1\alpha\Gamma_2\beta\Gamma_3} m(\alpha,\beta;\gamma)[\Gamma_1\gamma\Gamma_3]_k.$$

Here is an other point of view concerning the composition of Hecke operators. For Γ a congruence subgroup, let

$$\mathcal{M}_\Gamma := \mathbb{Z}[\Gamma\backslash \mathrm{GL}_2(\mathbb{Q})_+] = \bigoplus \mathbb{Z}[\Gamma\alpha].$$

It is the free abelian group generated by the left orbits of Γ acting on $\mathrm{GL}_2(\mathbb{Q})_+$. The group $\mathrm{GL}_2(\mathbb{Q})_+$ acts naturally by multiplication on the right on this $\mathbb{Z}$-module. Moreover the group $\mathrm{GL}_2(\mathbb{Q})_+$ acts transitively on a basis of this space containing the trivial class Γ. Consequently, a $\mathrm{GL}_2(\mathbb{Q})_+$-equivariant endomorphism of $\mathcal{M}_\Gamma$ is characterized by the image of the element $[\Gamma]$. As the stabilizer of this element is exactly Γ. It is not complicated to check that the submodule of Γ-invariant elements in $\mathcal{M}_\Gamma$ is exactly the submodule generated by the element of the form

$$\sum [\Gamma\alpha_i]$$

where $\coprod \Gamma\alpha_i$ is a double class of Γ in $\mathrm{GL}_2(\mathbb{Q})_+$. More precisely if $\Gamma\alpha\Gamma$ is a double class in $\mathrm{GL}_2(\mathbb{Q})_+$ let $[\Gamma\alpha\Gamma]$ be the element of $\mathcal{M}_\Gamma$ defined by

$$[\Gamma\alpha\Gamma] = \sum [\Gamma\alpha_i]$$

where $\coprod \Gamma\alpha_i$ is a decomposition of $\Gamma\alpha\Gamma$ in left classes. Let $\mathcal{R}(\Gamma)$ be the $\mathbb{Z}$-submodule of $\mathcal{M}_\Gamma$ generated by these double class elements. Then we have

Lemma 3.14. *We have an equality* $\mathcal{R}(\Gamma) = \mathcal{M}_\Gamma^\Gamma$ *and the map* $\phi \mapsto \phi([\Gamma])$ *induces an isomorphism*

$$\mathrm{End}_{\mathrm{GL}_2(\mathbb{Q})_+} \mathcal{M}_\Gamma \simeq \mathcal{R}(\Gamma).$$

This lemma implies that the $\mathbb{Z}$-module $\mathcal{R}(\Gamma)$ has actually a structure of ring with multiplication coming from the composition in $\mathrm{End}_{\mathrm{GL}_2(\mathbb{Q})_+} \mathcal{M}_\Gamma$. Let's determine explicitly this composition law. To determine the sum of double classes corresponding to the composite of $[\Gamma\alpha\Gamma]$ with $[\Gamma\beta\Gamma]$ it is sufficient to understand what is the image of $[\Gamma]$ by $[\Gamma\alpha\Gamma] \circ [\Gamma\beta\Gamma]$. It is exactly

$$\sum_{(i,j)} [\Gamma\alpha_i\beta_j] = \sum_{\Gamma\gamma\Gamma \subset \Gamma\alpha\Gamma\beta\Gamma} m(\alpha, \beta; \gamma)[\Gamma\gamma\Gamma].$$

Consequently the map

$$\mathcal{R}(\Gamma) \to \mathrm{End}_{\mathbb{C}}(M_k(\Gamma))$$

sending $[\Gamma\alpha\Gamma]$ on the Hecke operator $[\Gamma\alpha\Gamma]_k$ is a ring homomorphism.

Example of $\mathrm{SL}_2(\mathbb{Z})$ Let $\Gamma = \mathrm{SL}\,2(\mathbb{Z})$. We define $\mathcal{H}(\Gamma) \subset \mathrm{End}_{\mathrm{GL}_2(\mathbb{Q})_+} \mathcal{M}_\Gamma$ as the sub algebra generated by the double coset included in $\mathcal{M}_2(\mathbb{Z})$. It is the *abstract Hecke algebra* of group Γ.

In this case the $\mathbb{Z}$-module $\mathcal{M}_\Gamma$ can be identified with the free abelian ring with basis the set of lattices in $\mathbb{Q}^2$. Namely we make correspond a class $\Gamma\alpha$ to the lattice ${}^t\alpha\mathbb{Z}^2$.

The double classes of $\mathrm{SL}_2(\mathbb{Z})$ in $\mathcal{M}_2(\mathbb{Z})$ are in bijection with pairs of positive integers (d_1, d_2) such that $d_1 \mid d_2$. To (d_1, d_2) corresponds the double class of the diagonal matrix $\left(\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right)$. Let $T(d_1, d_2)$ be the element of $\mathcal{H}(\Gamma)$ corresponding to this double class and for $n \geqslant 1$, we define

$$T(n) = \sum_{d_1 d_2 = n} T(d_1, d_2).$$

The operator $T(n)$ corresponds to the formal sum of double classes of $\mathrm{SL}_2(\mathbb{Z})$ in $\mathcal{M}_2(\mathbb{Z})$ of determinant n. For $k \geqslant 2$, we define $T_k(n)$ and $T_k(d_1, d_2)$ their images in $\mathrm{End}_{\mathbb{C}} M_k(\Gamma)$.

Remark 3.15. The operator $T(n, n)$ is easy to compute : it corresponds to a double class generated by a central element, it is consequently a single left class and we have

$$T_k(n, n) = n^{k-2} I_{M_k(\Gamma)}.$$

Proposition 3.16. *In the abstract Hecke algebra, we have the equalities*

(i) If $m \wedge n = 1$, *then* $T(mn) = T(m)T(n)$;

(ii) if p *is prime and* $n \geqslant 1$, *we have*

$$T(p^n)T(p) = T(p^{n+1}) + pT(p, p)T(p^{n-1});$$

(iii) for general $m \geqslant 1$ and $n \geqslant 1$ we have

$$T(m)T(n) = \sum_{\substack{d|m\wedge n \\ d\geqslant 1}} dT(d,d)T\left(\frac{mn}{d^2}\right).$$

Proof. It is sufficient to understand the action of $T(n)$ on the space $\mathcal{M}_\Gamma$ identified to the $\mathbb{Z}$-module of lattices in $\mathbb{Z}^2$. If $\alpha \in \mathcal{M}_2(\mathbb{Z})$, we have $\det \alpha = n$ if and only if the lattice ${}^t\alpha\mathbb{Z}^2$ is of index n in $\mathbb{Z}^2$. Consequently we have the formula, for a lattice Λ in $\mathbb{Q}^2$.

$$T(n)[\Lambda] = \sum_{\substack{\Lambda'\subset\Lambda \\ [\Lambda:\Lambda']=n}} [\Lambda'].$$

The first formula is then a consequence of the fact that if $m \wedge n = 1$, and $\Lambda'' \subset \Lambda$ is sublattice of index mn, there exists a unique intermediate lattice $\Lambda'' \subset \Lambda' \subset \Lambda$ such that $[\Lambda : \Lambda'] = n$. The second formula can be proved by some analogous reasoning and the third formula is a consequence of the first two. □

Corollary 3.17. *The algebra $\mathcal{H}(\Gamma)$ is commutative and so are $\mathcal{H}_k(\Gamma)$ for all $k \geqslant 2$.*

From the commutativity, there is no danger to write $T_k(m)(f)$ for $f \mid T_k(m)$.

We can now compute the effect of Hecke operators on the q-development of modular forms for $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 3.18. *Let $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ and let $\sum_{n\geqslant 0} a_n(f)q^n$ be its q-development. For $m \geqslant 1$, we have*

$$T_k(m)(f) = \sum_{n\geqslant 0} a_n(T_k(m)f)q^n$$

with

$$a_n(T_k(m)f) = \sum_{\substack{a|m\wedge n \\ a\geqslant 1}} a^{k-1} a_{\frac{mn}{a^2}}(f).$$

Proof. Let

$$\mathcal{S}_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = n,\ 0 \leqslant b < d \right\}.$$

The map $g \mapsto {}^t g\mathbb{Z}^2$ induces a bijection from $\mathcal{S}_n$ on the set of lattices in $\mathbb{Z}^2$ of index n, so that

$$T_k(n) = \sum_{g\in\mathcal{S}_n} [g]_k.$$

The result follows from a direct computation. □

Example 3.19. If p is a prime, we have

$$T_k(p)(\sum_{n\geqslant 0} a_n q^n) = \sum_{n\geqslant 0} a_{pn} q^n + p^{k-1} \sum_{n\geqslant 0} a_n q^{pn}.$$

3.5 Adelic quotients

Let $\mathbb{A}_{\mathbb{Q}}$ be the ring of *adeles* of $\mathbb{Q}$. Let $\mathcal{P}$ be the set of prime numbers in $\mathbb{Q}$. By definition $\mathbb{A}_{\mathbb{Q}}$ is the ring

$$\mathbb{A}_{\mathbb{Q}} = \{(x_v) \in \prod_{v \in \mathcal{P} \cup \{\infty\}} \mathbb{Q}_v \mid \text{ for almost all } p \in \mathcal{P},\ x_v \in \mathbb{Z}_p\}.$$

It can be described as an inductive limit over finite subsets $S \subset \mathcal{P}$:

$$\mathbb{A}_{\mathbb{Q}} = \varinjlim_{S} (\prod_{p \in S} \mathbb{Q}_p \prod_{p \notin S} \mathbb{Z}_p \times \mathbb{R}).$$

We consider the inductive limit topology on this set where each product $\prod_{p\in S} \mathbb{Q}_p \prod_{p\notin S} \mathbb{Z}_p \times \mathbb{R}$ is endowed with the product topology. The topology of $\mathbb{A}_{\mathbb{Q}}$ has a basis whose elements are the $\prod_{p\in\mathcal{P}} U_p \prod_{p\notin S} \mathbb{Z}_p \times]a,b[$ for S a finite subset of $\mathcal{P}$, U_p an open subset of $\mathbb{Q}_p$ and $a < b$ two real numbers.

For this topology, the ring $\mathbb{A}_{\mathbb{Q}}$ is a topological ring. The diagonal injection $\mathbb{Q} \to \mathbb{A}_{\mathbb{Q}}$ is a morphism of rings whose image is discrete in $\mathbb{A}_{\mathbb{Q}}$. We use this injection to identify $\mathbb{Q}$ to a discrete subring of $\mathbb{A}_{\mathbb{Q}}$. It can be checked that the quotient $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact and isomorphic, as a topologique group, to $\prod_p \mathbb{Z}_p \times (\mathbb{R}/\mathbb{Z})$.

Let $\mathbb{A}_{\mathbb{Q}}^f \subset \mathbb{A}_{\mathbb{Q}}$ be the closed subring of elements $(x_v)_{v\in\mathcal{P}\cup\{\infty\}}$ such that $x_\infty = 0$. It is called the subring of *finite adeles*. Let $\widehat{\mathbb{Z}}$ be the profinite completion of $\mathbb{Z}$, ie $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. There is a decomposition $\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$ identifying $\widehat{\mathbb{Z}}$ to an open subring of $\mathbb{A}_{\mathbb{Q}}^f$.

The field $\mathbb{Q}$ injects diagonally in $\mathbb{A}_{\mathbb{Q}}^f$: $\mathbb{Q} \to \mathbb{A}_{\mathbb{Q}}^f$. We have to be careful here : the two diagonal injections $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}^f$ and $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$ are not compatible ! We have an equality $\mathbb{A}_{\mathbb{Q}}^f = \mathbb{Q} + \widehat{\mathbb{Z}}$. As $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$, we conclude that $\mathbb{Q}$ is dense in $\mathbb{A}_{\mathbb{Q}}^f$.

The group of invertible elements $\mathbb{A}_{\mathbb{Q}}^\times$ is the set of elements (x_v) such that $x_p \in \mathbb{Z}_p^\times$ excepted for a finite number of primes p. More generally, if $n \geqslant 1$, we define $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ as the set of invertible matrices of $\mathcal{M}_n(\mathbb{A}_{\mathbb{Q}})$. It can be described as the set

$$\left\{(g_v) \in \prod_v \mathrm{GL}_n(\mathbb{Q}_v) \mid g_p \in \mathrm{GL}_n(\mathbb{Z}_p) \text{ for almost all primes } p\right\}.$$

This is indeed a generalisation since $\mathbb{A}_{\mathbb{Q}}^\times = \mathrm{GL}_1(\mathbb{A}_{\mathbb{Q}})$. In order to define a topology on these sets, we embed $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ into $\mathcal{M}_n(\mathbb{A}_{\mathbb{Q}}) \times \mathbb{A}_{\mathbb{Q}}$ via the map $M \mapsto (M, \det(M)^{-1})$. Its image is a closed subset of $\mathcal{M}_n(\mathbb{A}_{\mathbb{Q}}) \times \mathbb{A}_{\mathbb{Q}}$ since it is the set of pairs (M, a) such that $a\det(M) = 1$. We consider the topology on $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ which is induced by the product topology of $\mathcal{M}_n(\mathbb{A}_{\mathbb{Q}}) \times \mathbb{A}_{\mathbb{Q}}$ on $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$. A base for this topology is given by the subsets

$$\prod_{p\in S} U_p \prod_{p\notin S} \mathrm{GL}_n(\mathbb{Z}_p) \times U_\infty$$

where S is a finite set of prime numbers, U_p is an open subset of $\mathrm{GL}_n(\mathbb{Q}_p)$ and U_∞ is an open subset of $\mathrm{GL}_2(\mathbb{R})$. For example the group $\mathrm{GL}_n(\widehat{\mathbb{Z}}) \simeq \prod_p \mathrm{GL}_n(\mathbb{Z}_p)$ is an open and compact subgroup of $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}}^f)$. Moreover we have a decomposition of topological groups $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}}) \simeq \mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}}^f) \times \mathrm{GL}_n(\mathbb{R})$. The image of the diagonal embedding $\mathrm{GL}_n(\mathbb{Q}) \hookrightarrow \mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ is discrete.

Now we consider especially the case where $n = 2$. We endow the group $\mathrm{SL}_2(\mathbb{A}_{\mathbb{Q}}^f)$ with the topology induced by the topology of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f)$. Note that it is also the topology induced from the inclusion (with closed image) $\mathrm{SL}_2(\mathbb{A}_{\mathbb{Q}}^f) \subset \mathcal{M}_2(\mathbb{A}_{\mathbb{Q}}^f)$.

Lemma 3.20. *The diagonal inclusion $\mathrm{SL}_2(\mathbb{Q}) \subset \mathrm{SL}_2(\mathbb{A}_{\mathbb{Q}}^f)$ has a dense image.*

Proof. For any ring A, the map

$$\begin{array}{ccc} A^3 & \longrightarrow & \mathrm{SL}_2(A) \\ (x,y,z) & \longmapsto & \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \end{array}$$

is surjective. Replacing A with $\mathbb{A}_{\mathbb{Q}}^f$, we obtain a continuous and surjective map $(\mathbb{A}_{\mathbb{Q}}^f)^3 \to \mathrm{SL}_2(\mathbb{A}_{\mathbb{Q}}^f)$. The image of $\mathbb{Q}^3$ under this map is exactly $\mathrm{SL}_2(\mathbb{Q})$. The desired result is then a consequence of the density of $\mathbb{Q}$ inside $\mathbb{A}_{\mathbb{Q}}^f$. □

Lemma 3.21. *We have $\mathbb{A}_{\mathbb{Q}}^\times = \mathbb{Q}_+^\times \widehat{\mathbb{Z}}^\times$. If $H \subset (\mathbb{A}_{\mathbb{Q}}^f)$ is a compact open subgroup of $\mathbb{A}_{\mathbb{Q}}^f$, the quotient $(\mathbb{A}_{\mathbb{Q}}^f)^\times / \mathbb{Q}_+^\times H$ is finite.*

Proof. The first assertion is a direct consequence of the fact that $\mathbb{Z}$ is a PID. For the second assertion, we remark that H is a subgroup of the maximal compact subgroup $\widehat{\mathbb{Z}}^\times$. As H is open in $\widehat{\mathbb{Z}}^\times$, the quotient $\widehat{\mathbb{Z}}^\times / H$ is finite. It follows from the first assertion that $(\mathbb{A}_{\mathbb{Q}}^f)^\times / \mathbb{Q}_+^\times H$ is isomorphic to a quotient of $\widehat{\mathbb{Z}}^\times / H$. □

Lemma 3.22. *Let $K \subset \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f)$ be a compact open subgroup. Then the double quotient $\mathrm{GL}_2(\mathbb{Q})_+ \backslash \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f) / K$ is finite. Moreover if $\det(K) = \widehat{\mathbb{Z}}^\times$, this double quotient is a singleton. If $K \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we can write*

$$\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f) = \coprod_{i=1}^{r} \mathrm{GL}_2(\mathbb{Q})_+ g_i K$$

for finitely many $g_i \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Proof. We can consider the map $\mathrm{GL}_2(\mathbb{Q})_+ \backslash \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f) / K \to (\mathbb{A}_{\mathbb{Q}}^f)^\times / \mathbb{Q}^\times \det(K)$ induced by the determinant. Assume that x and y are two elements of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f)$ such that $\mathbb{Q}_+^\times \det(x) \det(K) = \mathbb{Q}_+^\times \det(y) \det(K)$. We want to prove that $\mathrm{GL}_2(\mathbb{Q})_+ xK = \mathrm{GL}_2(\mathbb{Q})_+ yK$.

As $\det(\mathrm{GL}_2(\mathbb{Q})_+) = \mathbb{Q}_+^\times$, we can assume that $\det(x) = \det(y)$. Multiplying by y^{-1} on the right, it is sufficient to prove that $\mathrm{GL}_2(\mathbb{Q})_+ xy^{-1}(yKy^{-1}) = \mathrm{GL}_2(\mathbb{Q})(yKy^{-1})$. Now $xy^{-1} \in \mathrm{SL}_2(\mathbb{A}_\mathbb{Q}^f)$ and we deduce from Lemma 3.20, that $\mathrm{SL}_2(\mathbb{A}_\mathbb{Q}^f) = \mathrm{SL}_2(\mathbb{Q})((yKy^{-1}) \cap \mathrm{SL}_2(\mathbb{A}_\mathbb{Q}^f))$ since $yKy^{-1} \cap \mathrm{SL}_2(\mathbb{A}_\mathbb{Q}^f))$ is an open subgroup of $\mathrm{SL}_2(\mathbb{A}_\mathbb{Q}^f)$.

We can remark that a continuous morphism $G \to H$ between topological groups having a continuous section $s : H \to G$ is open. This is the case of det, a section being given by $x \mapsto \left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Consequently the group $\det(K)$ is compact and open inside $\mathbb{A}_\mathbb{Q}^f$. It is consequently contained in $\widehat{\mathbb{Z}}^\times$. The finiteness and the last assertion are consequence of Lemma 3.21. □

Let $K \subset \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f)$ be a compact open subgroup. Up to conjugation, we can assume that $K \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ which we always do in the sequel. Let $K_\infty \coloneqq \mathrm{O}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$. It is a maximal compact subgroup and let $K_\infty^\circ \coloneqq \mathrm{SO}_2(\mathbb{R})$ be its neutral component (the connected component of the neutral element).

We define

$$X_K \coloneqq \mathrm{GL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) / (KK_\infty).$$

The introduction of this double quotient is easily justified by the analogy with class field theory (that we can recover by replacing GL_2 with GL_1). As KK_∞ is compact and $\mathrm{GL}_2(\mathbb{Q})$ is discrete, the topological space X_K is locally compact. Let $X_\infty \coloneqq \mathrm{GL}_2(\mathbb{R})/K_\infty$ which is locally compact topological space. As K_∞ contains matrices of negative determinant, the action of $\mathrm{GL}_2(\mathbb{R})_+$ is transitive on X_∞. Consequently we have an homeomorphism

$$X_K \simeq \mathrm{GL}_2(\mathbb{Q})_+ \backslash (X_\infty \times \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f)/K).$$

Using Lemma 3.22, we see that there exists $g_1, \dots, g_r \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that

$$X_K = \coprod_{i=1}^r \Gamma_i \backslash X_\infty$$

where $\Gamma_i = \mathrm{GL}_2(\mathbb{Q})_+ \cap g_i K g_i^{-1} \subset \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f)$. As $g_i \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have

$$\Gamma_i \subset \mathrm{GL}_2(\mathbb{Q})_+ \cap \mathrm{GL}_2(\widehat{\mathbb{Z}}) = \mathrm{SL}_2(\mathbb{Z}).$$

Moreover, a basis of neighborhoods of 1 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is given by the subgroups $K(N) = \mathrm{Ker}(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}))$ with $N \geqslant 1$. As K is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, there exists some $N \geqslant 1$ such that $K(N) \subset K$. As $\mathrm{GL}_2(\mathbb{Q})_+ \cap K(N) = \Gamma(N)$, we must have $\Gamma(N) \subset \Gamma_i$ for all $1 \leqslant i \leqslant r$ showing that the groups Γ_i are actually congruences subgroups.

The space X_∞ is almost really Poincaré upper half plane $\mathbb{H}$. Namely stabiliser of i in $\mathrm{GL}_2(\mathbb{R})_+$ for his action on $\mathbb{H}$ is the subgroup of similitudes $Z(\mathbb{R})\,\mathrm{SO}_2(\mathbb{R})$ with Z the center of $\mathrm{GL}_2(\mathbb{R})$. There is a isomorphism of topological group $A_\infty \times \mathrm{O}_2(\mathbb{R}) \simeq Z(\mathbb{R})\,\mathrm{SO}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})_+$, where $A_\infty \simeq \mathbb{R}_+^\times$ is the neutral component of $Z(\mathbb{R})$, inducing

a diffeomorphism $A_\infty \times \mathbb{H} \simeq X_\infty$. As A_∞ is actually contained in the center of $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ and since $\mathrm{GL}_2(\mathbb{Q})_+ \cap K \times A_\infty = \{1\}$, we obtain a diffeomorphism

$$A_\infty \times \left(\coprod_{i=1}^{r} Y(\Gamma_i) \right) \simeq X_K.$$

The space X_K is consequently "almost" a disjoint union of modular curves $Y(\Gamma_i)$. If we assume moreover that $\det(K) = \widehat{\mathbb{Z}}^\times$, then $r = 1$ and

$$A_\infty \times Y(\Gamma) \simeq X_K = \mathrm{GL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) / (K \times O_2(\mathbb{R}))$$

where Γ is the congruence subgroup $\mathrm{GL}_2(\mathbb{Q})_+ \cap K$.

Example 3.23. For $N \geqslant 1$ define

$$K_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \mid c \in N\widehat{Z} \right\}, \quad K_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K_0(N) \mid a - 1 \in N\widehat{Z} \right\}.$$

Both $K_0(N)$ and $K_1(N)$ are compact open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Moreover $\Gamma_0(N) = \mathrm{GL}_2(\mathbb{Q})_+ \cap K_0(N)$ and $\Gamma_1(N) = \mathrm{GL}_2(\mathbb{Q})_+ \cap K_1(N)$. Consequently we have isomorphisms

$$X_{K_0(N)}/A_\infty \simeq Y_0(N), \quad X_{K_1(N)}/A_\infty \simeq Y_1(N).$$

The groups $K_0(N)$ and $K_1(N)$ can be decomposed as products indexed by prime numbers $K_i(N) = \prod_p K_i(N)_p$ where $K_i(N)_p$ is the compact open subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ defined by

$$K_0(N)_p = \left\{ M \mid M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ [p]^{v_p(N)} \right\}$$
$$K_i(N)_p = \left\{ M \mid M \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \ [p]^{v_p(N)} \right\}.$$

If $K \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f) = \mathrm{GL}_2(\mathbb{Q})_+ K$ so that the inclusion $\mathrm{GL}_2(\mathbb{Q}) \subset \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f)$ induces two bijections

$$\Gamma \backslash \mathrm{GL}_2(\mathbb{Q})_+ \xrightarrow{\sim} K \backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f),$$
$$\Gamma \backslash \mathrm{GL}_2(\mathbb{Q})_+ / \Gamma \xrightarrow{\sim} K \backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f) / K.$$

Moreover if K is a product $\prod_p K_p$ with K_p a compact open subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$, then we have

$$K \backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f) \simeq \varinjlim_{S \subset \mathcal{P}} \prod_{p \in S} K_p \backslash \mathrm{GL}_2(\mathbb{Q}_p),$$
$$K \backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^f) / K \simeq \varinjlim_{S \subset \mathcal{P}} \prod_{p \in S} K_p \backslash \mathrm{GL}_2(\mathbb{Q}_p) / K_p$$

where S is a finite subset of $\mathcal{P}$. These isomorphisms are induced by injections

$$\begin{array}{ccc} \prod_{p\in S} K_p\backslash \mathrm{GL}_2(\mathbb{Q}_p)/K_p & \longrightarrow & K\backslash \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f)/K \\ \prod_{p\in S} K_p g_p & \longmapsto & K\iota_S(g) \end{array}$$

where $\iota_S(g)$ is the element $h \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f)$ such that $h_p = g_p$ if $p \in S$ and $h_p = 1$ if $p \notin S$. In particular we have a injection of rings

$$\mathbb{Z}\left[K_p\backslash \mathrm{GL}_2(\mathbb{Q}_p)/K_p\right] \hookrightarrow \mathbb{Z}\left[K\backslash \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f)/K\right].$$

Note $\mathcal{R}(K_p) = \mathbb{Z}[K_p\backslash \mathrm{GL}_2(\mathbb{Q}_p)/K_p]$ is a ring after identification with the set of $\mathrm{GL}_2(\mathbb{Q}_p)$-equivariant endomorphisms of $\mathbb{Z}[K_p\backslash \mathrm{GL}_2(\mathbb{Q}_p)]$.

To summarise, we have an isomorphism of rings

$$\varinjlim_{S\subset\mathcal{P}} \left(\bigotimes_{p\in S} \mathcal{R}(K_p)\right) \simeq \mathcal{R}(\Gamma)$$

where $\mathcal{R}(K_p) = \mathbb{Z}[K_p\backslash \mathrm{GL}_2(\mathbb{Q}_p)/K_p]$ and $\Gamma = \mathrm{GL}_2(\mathbb{Q})_+ \cap \prod_p K_p$.

3.6 Hecke operators for more general congruence subgroups

Now we fix $N \geqslant 1$ et we define $\Gamma = \Gamma_1(N)$. We have to be more careful when defining Hecke algebras if we want to keep having commutative algebras. Let

$$\Delta_1(N) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})_+ \mid N \mid c,\ a \equiv 1\,[N] \text{ and } d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

Moreover we denote Δ_N the subset of $\mathcal{M}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})_+$ consisting of matrices of determinant prime to N.

Proposition 3.24. *The inclusion $\Delta_1(N) \subset \Delta$ induces a bijection*

$$\Gamma_1(N)\backslash\Delta_1(N)/\Gamma_1(N) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})\backslash\Delta_N/\mathrm{SL}_2(\mathbb{Z}). \tag{3}$$

Let $\mathcal{H}^{(N)}(\Gamma_1(N))$ be the subalgebra of $\mathcal{R}(\Gamma_1(N))$ generated by elements $[\Gamma_1(N)\alpha\Gamma_1(N)]$ with $\alpha \in \Delta_1(N)$. The map $[\Gamma_1(N)\alpha\Gamma_1(N)] \mapsto [\mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z})]$ induces an injective morphism of rings

$$\mathcal{H}^{(N)}(\Gamma_1(N)) \hookrightarrow \mathcal{H}(\mathrm{SL}_2(\mathbb{Z}))$$

whose image is generated by element $T(n)$ and $T(m,m)$ with n and m prime to N.

Proof. Let $\alpha \in \Delta_1(N)$ and $(\alpha_p)_{p\in\mathcal{P}}$ its image in $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^f)$. If $p \nmid N$, then $K_1(N)_p = \mathrm{GL}_2(\mathbb{Z}_p)$ so that

$$K_1(N)_p\alpha_p K_1(N)_p = \mathrm{GL}_2(\mathbb{Z}_p)\alpha_p\,\mathrm{GL}_2(\mathbb{Z}_p).$$

If $p \mid N$, then $\alpha_p \in K_1(N)_p$ so that

$$K_1(N)_p \alpha_p K_1(N)_p = K_1(N)_p, \quad \mathrm{GL}_2(\mathbb{Z}_p)\alpha_p \,\mathrm{GL}_2(\mathbb{Z}_p).$$

This implies that, for α and β in $\Delta_1(N)$, we have

$$\mathrm{GL}_2(\widehat{\mathbb{Z}})\alpha \,\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \mathrm{GL}_2(\widehat{\mathbb{Z}})\beta \,\mathrm{GL}_2(\widehat{\mathbb{Z}}) \Rightarrow K_1(N)\alpha K_1(N) = K_1(N)\beta K_1(N).$$

This implies the injectivity of the map (3). (...) □

The algebra $\mathcal{H}^{(N)}(\Gamma_1(N))$ is consequently commutative and acts on $M_k(\Gamma_1(N))$ for all $k \geqslant 1$. We denote by $\mathcal{H}_k^{(N)}(\Gamma_1(N))$ its image in $\mathrm{End}_{\mathbb{C}}(M_k(\Gamma_1(N))$.

Let $d_1 \mid d_2$ be two elements of $\mathbb{N}$ such that $m = d_1 d_2$ is prime to N. Let $T(d_1, d_2)$ the element $\mathcal{H}^{(N)}(\Gamma_1(N))$ corresponding to the element of $\mathcal{H}(\mathrm{SL}_2(\mathbb{Z}))$ written with the same symbol. For n prime to N, we define

$$T(n) = \sum_{\substack{d_1 \mid d_2 \\ d_1 d_2 = n}} T(d_1, d_2).$$

It follows from proposition 3.24 that we have, for $p \nmid N$

$$T(p^k)T(p) = T(p^{k+1}) + pT(p,p)T(p^{k-1}).$$

More generally, if $T \in \mathrm{End}\,\mathcal{M}_\Gamma$, we denote by T_k the image of T in the ring of endomorphisms of $M_k(\Gamma)$.

Remark 3.25. We have to care to the fact that the operator $T(p,p)_k$ does not act on $M_k(\Gamma_1(N))$ by multiplication by p^{k-1}, contrary to the case of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 3.26. *Let $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and let $\alpha \in \Gamma_0(N)$ such that*

$$\alpha \equiv \begin{pmatrix} d^{-1} & * \\ 0 & d \end{pmatrix} [N].$$

We define $\langle d \rangle \in \mathcal{R}(\Gamma_1(N))$ the element corresponding to the double class $\Gamma_1(N)\alpha\Gamma_1(N)$. It is actually a simple class depending only on d.

Let $p \nmid N$ and let α_p defining $\langle p \rangle$. We have

$$p\alpha \equiv \begin{pmatrix} 1 & * \\ 0 & p^2 \end{pmatrix} [N]$$

and $\mathrm{SL}_2(\mathbb{Z})p\alpha \,\mathrm{SL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$. This implies that the element $T(p,p) \in \mathcal{H}^{(N)}(\Gamma_1(N))$ corresponds to the double class of the matrix $p\alpha$. Specializing in $\mathrm{End}\, M_k(\Gamma_1(N))$, we obtain the relation

$$T(p,p)_k = p^{k-1}\langle p \rangle_k$$

and

$$T(p^m)_k T(p)_k = T(p^{m+1})_k + p^{k-1}\langle p\rangle_k T(p^{m-1}).$$

Finally, if all prime divisors of $m \geqslant 1$ are also divisors of N (that we note $m \mid N^\infty$) we define

$$T(m) = [\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & m\end{pmatrix}\Gamma_1(N)] \in \mathcal{R}(\Gamma_1(N))$$

and we define $\mathcal{H}(\Gamma_1(N))$ as the sub-algebra of $\mathcal{R}(\Gamma_1(N))$ generated by $\mathcal{H}^{(N)}(\Gamma_1(N))$ and all other operators $\langle d\rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $T(m)$ for $m \mid N^\infty$.

Theorem 3.27. *Let $m \geqslant 1$ and let $m = m'm''$ with m' prime to N and $m'' \mid N^\infty$. Then $T(m')T(m'') = T(m'')T(m')$. Moreover the algebra $\mathcal{H}(\Gamma_1(N))$ is commutative and generated by elements $T(n)$, $n \geqslant 1$ and $\langle d\rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.*

Proof. See [Shi, Thm. 3.34]. □

Action of Hecke operators on q-developments

Theorem 3.28. *Let $f \in M_k(\Gamma_1(N))$ be a modular form with q-development*

$$f(z) = \sum_{n\geqslant 0} c_n(f)q^n.$$

Then, for $m \geqslant 1$, we have

$$(f \mid T(m)_k)(z) = \sum_{n\geqslant 0} c_n(f \mid T(m)_k)q^n$$

with

$$c_n(f \mid T(m)_k) = \sum_{d\mid n\wedge m} d^{k-1} c_{\frac{mn}{d^2}}(\langle d\rangle_k f)$$

with the convention that $\langle d\rangle = 0$ if $d \wedge N \neq 1$.

Proof. See for example [Shi, p. 80]. □

Let χ be some character of $(\mathbb{Z}/N\mathbb{Z})^\times$. We define $M_k(\Gamma_1(N), \chi)$ as the χ-isotypic subspace of $M_k(\Gamma_1(N))$ for the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ defined by operators $\langle d\rangle$. More precisely

$$M_k(\Gamma_1(N), \chi) = \{f \in M_k(\Gamma_1(N)) \ \mid \langle d\rangle f = \chi(d)f\}.$$

As a particular case, we can check that $M_k(\Gamma_0(N)) = M_k(\Gamma_1(N), \chi_0)$ with χ_0 the trivial character. As an example, we obtain, for $f \in M_k(\Gamma_1(N), \chi)$,

$$T(p)_k f = \begin{cases} \sum_{n\geqslant 0} a_{pn}(f)q^n + p^{k-1}\chi(p)\sum_{n\geqslant 0} a_n(f)q^{np} & \text{if } p \nmid N \\ \sum_{n\geqslant 0} a_{pn}(f)q^n & \text{if } p \mid N. \end{cases}$$

3.7 Petersson inner product

On Poincaré upper half space $\mathbb{H}$, we have the hyperbolic measure $\mathrm{d}\mu(x+iy) = \frac{\mathrm{d}x\,\mathrm{d}y}{y^2}$. This measure is invariant under the action of the group $\mathrm{GL}_2(\mathbb{R})_+$. The fundamental domain $\mathcal{D} = \{z \in \mathbb{H} \mid |z| \geqslant 1, |\mathrm{Re}\, z| \leqslant 1/2\}$ has a finite volume for this measure.

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be some congruence subgroup. We can construct a fundamental domain for the action of Γ by defining

$$\mathcal{D}_\Gamma = \cup_\gamma \gamma(\mathcal{D})$$

with γ varying in among representants of $\Gamma\{\pm I_2\}\backslash \mathrm{SL}_2(\mathbb{Z})$.

Let φ be some function defined on $Y(\Gamma) = \Gamma\backslash\mathbb{H}$. We say that φ is *integrable* if φ is measurable and if the integral

$$\int_{\mathcal{D}_\Gamma} |\varphi|\,\mathrm{d}\mu = \sum_{j=1}^{r} \int_{\mathcal{D}} |\phi(\alpha_i -)|\,\mathrm{d}\mu$$

is convergent (with $\mathrm{SL}_2(\mathbb{Z}) = \coprod_{j=1}^r \Gamma\alpha_j$). We define

$$\mathrm{Vol}(\Gamma) \coloneqq \int_{\mathcal{D}_\Gamma} \mathrm{d}\mu = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma\{\pm I_2\}] \int_{\mathcal{D}} \mathrm{d}\mu.$$

Theorem 3.29. *Let $f \in M_k(\Gamma)$ and let $g \in S_k(\Gamma)$. Then the function*

$$z \mapsto f(z)\overline{g(z)}\,\mathrm{Im}(z)^k$$

is integrable and the formula

$$\langle f, g\rangle = \mathrm{Vol}(\Gamma)^{-1} \int_{\mathcal{D}_\Gamma} f(z)\overline{g(z)}\,\mathrm{Im}(z)^k\,\mathrm{d}\mu$$

defines an hermitian inner product which is invariant under the action of Γ.

Proof. See for example [DS, §5.4]. □

The normalization of the inner product implies that, if $\Gamma' \subset \Gamma$, the injection $S_k(\Gamma) \subset S_k(\Gamma')$ is isometric. Consequently we obtain some inner product on $\widetilde{S}_k$.

Lemma 3.30. *Let $\alpha \in \mathrm{GL}_2(\mathbb{Q})_+$ and let $\alpha' = (\det\alpha)\alpha^{-1}$. Then we have, for f and g in $\widetilde{S}_k$,*

$$\langle f[\alpha]_k, g\rangle = \langle f, g[\alpha']_k\rangle.$$

Proof. This is [DS, Prop. 5.5.2]. □

From this lemma, we can deduce :

Proposition 3.31. *Let Γ be a congruence subgroup. For $f \in S_k(\Gamma)$ and $g \in S_k(\Gamma)$, we have*

$$\langle f[\Gamma\alpha\Gamma], g\rangle = \langle f, g[\Gamma\alpha'\Gamma]\rangle.$$

Corollary 3.32. *For $n \wedge N = 1$, the endomorphism $T(n)_k$ of $S_k(\Gamma_1(N))$ is normal. Moreover we have, $\langle d\rangle^* = \langle d^{-1}\rangle$.*

We can deduce from this corollary and from the commutativity of the algebra $\mathcal{H}(\Gamma_1(N))$ that the space $S_k(\Gamma_1(N))$ has an orthogonal basis in which all the operators $T(n)_k$ for $n \wedge N = 1$ and $\langle d\rangle$ are diagonal.

The case of $\mathrm{SL}_2(\mathbb{Z})$ is particular. Namely in this case, the space $S_k(\mathrm{SL}_2(\mathbb{Z}))$ has a unique such base. Namely each eigenspace for the action of $\mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}))$ is one dimensional. This can be checked by the formula $c_1(f \mid T(n)_k) = c_n(f)$ for $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$.

3.8 Old forms and newforms

Let $1 \leqslant M \mid N$ with $N = dM$ and let $\alpha_d := \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We have $\alpha_d^{-1}\Gamma_1(M)\alpha_d \subset \Gamma_1(N)$ which implies that

$$f \in S_k(\Gamma_1(M)) \Rightarrow f[\alpha_d]_k \in S_k(\Gamma_1(N)).$$

More generally, for $d \mid N$, we define a map

$$i_d : \begin{array}{ccc} S_k(\Gamma_1(N/d))^2 & \to & S_k(\Gamma_1(N)) \\ (f, g) & \mapsto & f + g[\alpha_d]_k. \end{array}$$

The subspace of *old forms* in $S_k(\Gamma_1(N))$ is the subspace generated by the images of all i_d for $d \mid N$, $d > 1$.

$$S_k(\Gamma_1(N))^{\mathrm{old}} := \sum_{\substack{d|N \\ d>1}} \mathrm{Im}(i_d).$$

It is easily checked that we have

$$S_k(\Gamma_1(N))^{\mathrm{old}} = \sum_{p|N} \mathrm{Im}(i_p).$$

The subspace of *newforms* is the orthogonal of the space of old forms for Petersson inner product

$$S_k(\Gamma_1(N))^{\mathrm{new}} := (S_k(\Gamma_1(N))^{\mathrm{old}})^{\perp}.$$

Proposition 3.33. *The subspaces $S_k(\Gamma_1(N))^{\mathrm{old}}$ and $S_k(\Gamma_1(N))^{\mathrm{new}}$ of $S_k(\Gamma_1(N))$ are stable under the action of the Hecke algebra $\mathcal{H}_k(\Gamma_1(N))$.*

Proof. See [DS, Prop. 5.6.2]. □

The main technical result of the theory of newforms is the following. A complete proof is in [DS] (see [DS, Thm. 5.7.1]).

Lemma 3.34. *Let $f \in S_k(\Gamma_1(N))$ be such that $a_n(f) = 0$ when $n \wedge N = 1$, then we can write $f = \sum_{p|N} i_p(f_p)$ with $f_p \in S_k(\Gamma_1(N/p))$.*

Let $f \in S_k(\Gamma_1(N))^{\text{new}}$ be a new form which is an eigenvector for operators $T(n)$ for $n \wedge N = 1$. It follows from the explicit action of Hecke operators on q-development that

$$a_n(f) = a_1(T_k(n)f) = \psi(T_k(n))a_1(f).$$

We deduce from Lemma 3.34 that $f \neq 0$ implies $a_1(f) \neq 0$ and that f is unique up to a scalar. This implies that f is an eigenvectors of all other elements of $\mathcal{H}_k(\Gamma_1(N))$. A newform which is an eigenvector for all $T(n)$, $n \wedge N = 1$ is called *proper*. Moreover if $a_1(f) = 1$, we say that f is *normalized*. Consequently we proved :

Theorem 3.35 (Atkin-Lehner)**.** *The $\mathbb{C}$-vector space $S_k(\Gamma_1(N))^{\text{new}}$ has a basis of common eigenvectors for the operators $T(n)$ and $\langle d \rangle$ when $n \wedge N = 1$ and $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Moreover each common eigenspace has dimension 1 and is generated by a unique normalized proper newform.*

This theorem of Atkin and Lehner is usually called "weak multiplicity one theorem". The "strong multiplicity one theorem" is a bit more involved. Here is its statement :

Theorem 3.36 (Atkin-Lehner)**.** *Let $f \in S_k(\Gamma_1(N))^{\text{new}}$ and $g \in S_k(\Gamma_1(M))^{\text{new}}$ be two proper forms corresponding to systems of eigenvalues*

$$\psi_f : \mathcal{H}_k(\Gamma_1(N)) \to \mathbb{C}, \quad \psi_g : \mathcal{H}_k(\Gamma_1(M)) \to \mathbb{C}.$$

Assume that $\psi_f(T(p)) = \psi_g(T(p))$ for all prime number p except a finite number of them. Then $N = M$ and $f = g$.

This theorem implies that if $\psi : \mathcal{H}_k(\Gamma_1(N)) \to \mathbb{C}$ is a system of eigenvalues then it corresponds to a unique newform f in level $N_f \mid N$. This level N_f is called the *conductor* of ψ.

3.9 Hecke eigensystems

Let $\mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$ be the sub-$\mathbb{C}$-algebra of $\text{End}_{\mathbb{C}} M_k(\Gamma_1(N))$ generated by $\mathcal{H}_k(\Gamma_1(N))$. There is consequently a surjective map $\mathcal{H}_k(\Gamma_1(N)) \otimes \mathbb{C} \twoheadrightarrow \mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$. This map is not *a priori* a bijection.

Theorem 3.37. *Assume that $k \geqslant 1$. The $\mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$-module $M_k(\Gamma_1(N))' \coloneqq \text{Hom}_{\mathbb{C}}(M_k(\Gamma_1(N)), \mathbb{C})$ is free of rank 1.*

Corollary 3.38. *We have $\dim_{\mathbb{C}} \mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}} = \dim_{\mathbb{C}} M_k(\Gamma_1(N))$. Moreover each character of $\mathbb{C}$-algebra $\mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}} \to \mathbb{C}$ corresponds to a unique eigenform $f \in M_k(\Gamma_1(N))$.*

Proof. We consider the bilinear pairing

$$\begin{array}{ccc} \mathcal{H}_k(\Gamma_1(N)) \times M_k(\Gamma_1(N)) & \longrightarrow & \mathbb{C} \\ (T, f) & \longmapsto & c_1(f|T). \end{array}$$

This is a perfect pairing. Namely if $c_1(f|T) = 0$ for all $T \in \mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$, we have $c_n(f) = c_1(f|T_k(n)) = 0$ for all $n \geqslant 1$. This implies that f is constant but, since $k \geqslant 1$, we have $f = 0$. If $T \in \mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$ is such that forall $f \in M_k(\Gamma_1(N))$, we have $c_1(f|T) = 0$, then $c_n(f|T) = c_1(f|TT(n)) = c_1((f|T(n))|T) = 0$ for all $f \in M_k(\Gamma_1(N))$ and $n \geqslant 1$. As above, this implies that $f|T = 0$ for all $f \in M_k(\Gamma_1(N))$ and finally $T = 0$. The two spaces $\mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$ and $M_k(\Gamma_1(N))$ begin finitely dimensional over $\mathbb{C}$, this is enough to prove that the pairing is perfect. The pairing induces an isomorphism $\mathcal{H}_k(\Gamma_1(N)) \xrightarrow{\sim} M_k(\Gamma_1(N))'$ which is $\mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$-equivariant and this proves the claim. □

If $\lambda : \mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}} \to \mathbb{C}$ is a character, we define

$$M_k(\Gamma_1(N))[\lambda] \coloneqq \{f \in M_k(\Gamma_1(N)) \mid \forall T \in \mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}},\ f|T = \lambda(T)f\}.$$

We can also define the sub-$\mathbb{Z}$-algebra $h_k(\Gamma_1(N)) \subset \mathrm{End}_{\mathbb{C}} S_k(\Gamma_1(N))$ generated by the operators T_p and $\langle d \rangle$, the sub-$\mathbb{C}$-algebra $h_k(\Gamma_1(N))_{\mathbb{C}}$ generated by $h_k(\Gamma_1(N))$. The same proof shows that $S_k(\Gamma_1(N))_{\mathbb{C}}$ is a free $h_k(\Gamma_1(N))_{\mathbb{C}}$-module of rank 1.

We will admit the following result, which will be proved only for $S_2(\Gamma_1(N))$.

Theorem 3.39. *In $\mathbb{C}$-vector spaces $M_k(\Gamma_1(N))$ (resp. $S_k(\Gamma_1(N))$), there exists a sub-$\mathbb{Z}$-module generated by a basis of $M_k(\Gamma_1(N))$ (resp. $S_k(\Gamma_1(N))$) which is stable under the action of $\mathcal{H}_k(\Gamma_1(N))$.*

Corollary 3.40. *The $\mathbb{Z}$-algebras $\mathcal{H}_k(\Gamma_1(N))$ (resp. $\mathcal{H}_k(\Gamma_1(N))$) is a finite free $\mathbb{Z}$-module of rank $\dim_{\mathbb{C}} M_k(\Gamma_1(N))$ (resp. $\dim_{\mathbb{C}} S_k(\Gamma_1(N))$).*

Proof. Let L_k be a finite free $\mathbb{Z}$-module stable by $\mathcal{H}_k(\Gamma_1(N))$ such that $M_k(\Gamma_1(N)) \simeq L_k \otimes \mathbb{C}$. As L_k is torsion free, we have

$$\mathrm{End}_{\mathbb{C}} M_k(\Gamma_1(N)) \simeq \mathbb{C} \otimes \mathrm{End}_{\mathbb{Z}} L_k$$

which implies the isomorphism $\mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}} \simeq \mathbb{C} \otimes \mathcal{H}_k(\Gamma_1(N))$. □

This result has the following consequence. Let $f \in M_k(\Gamma_1(N))$ be an eigenform which is moreover normalised (ie that $c_1(f) = 1$). Then the coefficients $c_n(f)$ are algebraic integers and generate a finite extension of $\mathbb{Q}$ denoted K_f. Namely let $\lambda : \mathcal{H}_k(\Gamma_1(N)) \to \mathbb{C}$ be the character sending an operator T on the eigenvalue $\lambda(T)$. The image of λ in $\mathbb{C}$ is a subring which is a quotient of $\mathcal{H}_k(\Gamma_1(N))$ and consequently a finite free $\mathbb{Z}$-module. It generates a number field and its elements are algebraic integers.

Now let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\sigma \circ \lambda$ is an other character $\mathcal{H}_k(\Gamma_1(N)) \to \overline{\mathbb{Q}} \subset \mathbb{C}$. As $M_k(\Gamma_1(N))'$ is finite free of rank 1 over $\mathcal{H}_k(\Gamma_1(N))_{\mathbb{C}}$, the subspace $M_k(\Gamma_1(N))[\sigma \circ \lambda]$ is non zero, which means that it contains a unique normalised eigenform $\sigma(f)$. This form is called the *conjugate* of f under σ.

Remark 3.41. If $f \in M_k(\Gamma_0(N))$, the fact that the operators $T(n)$ for $n \wedge N = 1$ are autoadjoint and the strong multiplicity one theorem imply that K_f is totally real.

Example 3.42. Here are some explicit example in weight 2 :

$$h_2(\Gamma_0(23)) \simeq \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}], \quad h_2(\Gamma_0(29)) \simeq \mathbb{Z}[\sqrt{2}], \quad h_2(\Gamma_0(31)) \simeq \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}].$$

4 Some complement of algebraic geometry

4.1 Schemes and functors

Let X be a scheme. If A is a ring, we recall that the set of A-points of X is the set

$$X(A) \coloneqq \mathrm{Hom}(\mathrm{Spec}\, A, X).$$

Consequently a scheme gives rise to a covariant functor from the category of rings to the category of sets. The category of rings being antiequivalent to the category of affine schemes, it is equivalent to consider the contravariant functor $Y \mapsto \mathrm{Hom}(Y, X)$ from the category of affine schemes to the category of sets. More generally, given a scheme S, we can define the set of S-points of X by

$$X(S) \coloneqq \mathrm{Hom}(S, X).$$

A contravariant functor from a category $\mathcal{C}$ to the category of sets is called a *presheaf* on the category $\mathcal{C}$. The presheaves over a category $\mathcal{C}$ form a category denoted $\widehat{\mathcal{C}}$. The main interest of this construction is the following result.

Theorem 4.1 (Yoneda)**.** *Let $\mathcal{C}$ be a category. The functor from $\mathcal{C}$ to the category $\widehat{\mathcal{C}}$ sending X to the presheaf* $\mathrm{Hom}(-, X)$ *is fully faithfull.*

Consequently we can identify a scheme X with its functor of points $\mathrm{Hom}(-, X)$ over the whole category of schemes. Actually the case of schemes is more special and we can even identify a scheme X to its functor of points over the full subcategory of affine schemes. It is a consequence of Theorem 4.1 and of the following lemma.

Lemma 4.2. *Let X be a scheme and let $(U_i)_{i\in I}$ be a covering of X by affine open subschemes and, for each $(i,j) \in I^2$, let $(V_{i,j}^k)_{k\in I_{i,j}}$ be a covering og $U_i \cap U_j$ by affine open subschemes. The the following sequence of functors is exact*

$$\mathrm{Hom}(X, -) \to \prod_{i\in I} \mathrm{Hom}(U_i, -) \rightrightarrows \prod_{\substack{(i,j)\in I^2 \\ k\in I_{i,j}}} \mathrm{Hom}(V_{i,j}^k, -).$$

Consequently we obtain the following result.

Corollary 4.3. *Let* Sch *be the category of schemes and* $\widehat{\mathrm{Aff}}$ *the category of presheaves over the category* Aff *of affine schemes. Then the functor* $X \mapsto \mathrm{Hom}(-, X)$ *from* Sch *to* $\widehat{\mathrm{Aff}}$ *is fully faithful. More generally, if* S *is a scheme and* $\mathrm{Sch}_{/S}$ *and* $\mathrm{Aff}_{/S}$ *denote the categories of* S*-schemes and of* S*-schemes which are affine, then the functor from* $\mathrm{Sch}_{/S}$ *to* $\widehat{\mathrm{Aff}_{/S}}$ *defined by* $X \mapsto \mathrm{Hom}_S(-, X)$ *is fully faithful.*

In summary, we can identify a scheme (resp. an S-scheme) to its functor of points over the category of affine schemes (resp. S-schemes which are affine).

Definition 4.4. *Let* S *be a scheme. An* S*-group scheme is a contravariant functor* $G : \mathrm{Aff}_{/S}^{\mathrm{op}} \to \mathrm{Gr}$ *from the category of* S*-schemes which are affine to the category of groups whose underlying presheaf is a scheme.*

When G is a group scheme, we use the same symbol G to describe its underlying scheme. In other words, a group scheme is a scheme G such that, for each map $\mathrm{Spec}\, A \to S$, the set $G(A)$ has, functorially in A, a group structure.

If G is a group scheme, the multiplication maps $m_A : (G \times_S G)(A) \simeq G(A) \times G(A) \to G(A)$ induce a *multiplication morphism* $m : G \times_S G \to G$. The family $(e_A \in G(A))_A$ gives rise to a *neutral section* $e_S \in G(S)$. Moreover there exists an *inverse* map $i : G \to G$ corresponding to the inverse map on each $G(A)$. The data (m, e_S, i) encodes the structure of group scheme over G. We have to be careful to the fact that the set G itself is not a group !

Example 4.5. a) We can define a group scheme $\mathbb{G}_a$ by $\mathbb{G}_a(A) = (A, +)$ for each ring A. The underlying scheme is isomorphic to $\mathrm{Spec}\, \mathbb{Z}[T]$. The multiplication map m comes from the ring homomorphism $m^* : \mathbb{Z}[T] \to \mathbb{Z}[T] \otimes_{\mathbb{Z}} \mathbb{Z}[T]$ defined by $m^*(T) = 1 \otimes T + T \otimes 1$.

b) The multiplicative group $\mathbb{G}_m$ is defined by the formula $\mathbb{G}_m(A) = (A^\times, \times)$. We have $\mathbb{G}_m \simeq \mathrm{Spec}\, \mathbb{Z}[T, T^{-1}]$ and $m^*(T) = T \otimes T$.

c) A generalization of $\mathbb{G}_m$ is

$$\mathrm{GL}_N(A) = \{M \in \mathcal{M}_N(A) \mid \det(M) \in A^\times\}.$$

It is a group scheme since $\mathrm{GL}_N \simeq \mathrm{Spec}\, \mathbb{Z}[(T_{i,j})_{1 \leqslant i,j \leqslant n}, \det^{-1}]$.

d) If H is a finite group, we can define the *constant group scheme* $\underline{H}(A) = \{\pi_0(\mathrm{Spec}\, A) \to H\}$ with the obvious group structure coming from H. It is a group scheme corresponding to $\coprod_{h \in H} \mathrm{Spec}\, \mathbb{Z}$.

e) For $N \geqslant 1$, we can define $\mu_N(A) = \{x \in A \mid x^N = 1\}$. We have

$$\mu_N \simeq \mathrm{Spec}\, \mathbb{Z}[T]/(T^N - 1).$$

4.2 Unramified, smooth and étale morphisms

Definition 4.6. *Let $f : X \to S$ be a morphism of schemes. We say that f is* smooth *if, for all $x \in X$, there exists an open neighbourhood U of x, an open neighbourhood V of $s = f(x)$ and a closed immersion $i : U \hookrightarrow \mathbb{A}^n_V$ such that $f(U) \subset V$, $f|_U = p \circ i$ where p is the canonical projection $\mathbb{A}^n_V \to V$ and the schematic image of j is defined by an ideal generated by functions $g_1, \ldots, g_r$ on $\mathbb{A}^n_V$ such that*

$$\operatorname{rk}\left(\frac{\partial g_i}{\partial X_j}\right)_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant n}} = r. \qquad \begin{array}{ccc} U & \xrightarrow{\ j\ } & \mathbb{A}^n_V \\ & \searrow^{f|_U} & \downarrow p \\ & & V \end{array}$$

We have the following equivalent characterization of smooth morphisms.

Proposition 4.7. *A morphism $f : X \to S$ is smooth if and only if it is locally of finite presentation, flat and geometrically regular, which means that for each point $s \in S$ and each map $\operatorname{Spec} \overline{k} \to s$ with $\overline{k}$ an algebraic closed field, the scheme $X \times_S \operatorname{Spec} \overline{k}$ is regular.*

Proof. See [BLR90, Prop. 2.3.8] and [BLR90, Prop. 2.2.15]. □

It follows from the definition that, for a smooth morphism $f : X \to S$, the sheaf of $\mathcal{O}_X$-modules $\Omega^1_{X/S}$ is locally free of finite rank. It follows from Proposition 4.7 that its rank at a point $x \in X$ is equal to $\dim_x f^{-1}(f(x))$. This implies that the function $x \mapsto \dim_x f^{-1}(f(x))$ is locally constant when f is smooth. The function $x \mapsto \operatorname{rk} \Omega^1_{X/S,x} = \dim_x f^{-1}(f(x))$ is called the *relative dimension* of the smooth morphism f.

A morphism $f : X \to S$ is called *étale* if it is smooth of relative dimension 0.

Corollary 4.8. *A morphism $f : X \to S$ is étale if and only if it is locally of finite presentation, flat and $\Omega^1_{X/S} = 0$.*

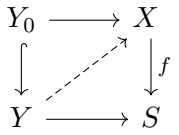
We say that a morphism $f : X \to S$ is *unramified* or *net* if it is locally of finite presentation and if $\Omega^1_{X/S} = 0$. In particular a morphism is étale if and only if it is flat and unramified if and only if it is smooth and unramified.

It is useful to have a characterization of unramified, smooth and étale morphism in terms of the functor of points.

Theorem 4.9. *Let $f : X \to S$ be a morphism locally of finite presentation. The map f is unramified (resp. smooth, resp. étale) if and only if for all S-scheme Y which is affine and for all closed subscheme $Y_0 \subset Y$ defined by some ideal I such that $I^2 = 0$, the map*

$$\operatorname{Hom}_S(Y, X) \longrightarrow \operatorname{Hom}_S(Y_0, X)$$

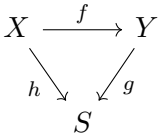
is injective (resp. surjective, resp. bijective).



Proof. See [BLR90, Prop. 2.2.6]. □

We deduce easily from this characterization that being unramified, smooth or étale is preserved by composition and base change.

Proposition 4.10. *Let $h : X \to S$ and $g : Y \to S$ be morphisms and $f : X \to Y$ a map of S-schemes. Assume that g is unramified. Then if h is smooth (resp. étale), so is f.*



Let $f : X \to S$ be a morphism of schemes and let $x \in X$. We say that f is unramified (resp. smooth, resp. étale) at x if it is so for $f|_U$ for some open neighbourhood U of x.

The smoothness of a morphism between smooth schemes can be read on the sheaves of differentials.

Proposition 4.11. *Let $f : X \to Y$ be a morphism between smooth S-schemes. Let $x \in X$. The following assertions are equivalent :*

(i) f is smooth at x ;

(ii) the morphism of $\mathcal{O}_{X,x}$-modules $(f^*\Omega^1_{Y/S})_x \to \Omega^1_{X/S,x}$ is injective and its image is a direct factor ;

(iii) the $k(x)$-linear map $(f^*\Omega^1_{Y/S}) \otimes k(x) \to \Omega^1_{X/S} \otimes k(x)$ is injective.

Proof. See [BLR90, Prop. 2.2.8]. □

Corollary 4.12. *Let $f : X \to Y$ be a morphism between smooth S-schemes. Let $x \in X$. The following assertions are equivalent :*

(i) f is étale at x ;

(ii) the morphism of $\mathcal{O}_{X,x}$-modules $(f^*\Omega^1_{Y/S})_x \to \Omega^1_{X/S,x}$ is an isomorphism ;

(iii) the $k(x)$-linear map $(f^*\Omega^1_{Y/S}) \otimes k(x) \to \Omega^1_{X/S} \otimes k(x)$ is bijective.

Corollary 4.13. *Let $f : X \to S$ be smooth of relative dimension r at $x \in X$. There exists an open neighbourhood U of x and a factorisation*

$$\begin{array}{ccc} U & \xrightarrow{g} & \mathbb{A}^n_S \\ & \searrow^{f|_U} & \downarrow p \\ & & S \end{array}$$

with g étale.

Example 4.14. a) Let L/K be a finite field extension. Then the map $\operatorname{Spec} L \to \operatorname{Spec} K$ is unramified if and only if L is a separable extension of K.

b) Let $A \subset B$ be complete discrete valuation ring. Then $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified if and only if k_B is a finite separable extension of k_A and an uniformizer of A is an uniformizer of B.

c) An immersion if unramified if and only if it is locally of finite presentation.

Example 4.15. a) Let S be a scheme and let $\mathcal{E}$ be a locally free sheaf of $\mathcal{O}_S$-modules. Then the map of schemes $\mathbb{V}(\mathcal{E}) \to S$ is smooth of relative dimension equal to the rank of $\mathcal{E}$.

b) Let k be a field of characteristic different from 2 and set $S = \operatorname{Spec} k[x]$, $X = \operatorname{Spec} k[x,y]/(y^2 - x)$. Then the map $X \to S$ is étale at each point different from the closed point $(0,0)$. Actually the map is ramified at $(0,0)$ since the localisation at (x,y) of $k[x,y]/(y^2 - x, x) \simeq k[y]/(y^2)$ is not reduced.

c) Let k be a field and set $S = k[z]$ and $X = k[x,y,z]/(xy - z)$. The map $X \to S$ is smooth of relative dimension 1 at all point excepted at $(0,0,0)$.

Definition 4.16. *Let G be some S-group scheme. We say that it is* finite flat *(resp.* finite étale*) if its underlying scheme is finite flat (resp.* finite étale*) over S.*

Example 4.17. a) Let H be a finite group. The constant group scheme $\underline{H}$ is obviously finite étale over $\operatorname{Spec} \mathbb{Z}$.

b) Let S be a scheme and let $\mu_{N,S} \coloneqq \mu_N \times S$. The S-group scheme $\mu_{N,S}$ is finite flat since $S[X]/(X^N - 1)$ is finite flat over S. However it is étale over S if and only if $N \in \mathcal{O}(S)^\times$. Namely we can assume that $S = \operatorname{Spec} A$ and consequently $\mu_{N,S} = \operatorname{Spec} B$ with $B = A[X]/(X^N - 1)$. Then $\mu_{N,S}$ is étale over S if and only if $\Omega^1_{B/A} = 0$. We have an exact sequence

$$(X^N - 1)/(X^N - 1)^2 \to \Omega^1_{A[X]/A} \otimes_A B \to \Omega^1_{B/A} \to 0.$$

The image of $X^N - 1$ in $\Omega^1_{A[X]/A} \simeq A[X]dX$ being $NX^{N-1}dX$. Consequently $\Omega^1_{B/A} = 0$ if and only if NX^{N-1} generates the $A[X]$-module $A[X]/(X^N - 1)$ which is equivalent to $N \in A^\times$. Namely assume that we can write

$$1 = Q_1(X)NX^{N-1} + Q_2(X)(X^N - 1).$$

Doing $X = 1$ shows that $N \in A^\times$. Conversely if $N \in A^{-1}$, we have $1 = -(X^N - 1) + N^{-1}X(NX^{N-1})$.

4.3 Cohomology and base change

Let $f : X \to S$ be a proper map of locally noetherian schemes. Then we know that, for each $n \geqslant 0$ and each coherent sheaf $\mathcal{F}$ on X, the sheaf $R^n f_* \mathcal{F}$ is coherent.

Proposition 4.18. *Let $S = \operatorname{Spec} A$ be some affine noetherian scheme and let $f : X \to S$ be a proper map. Let $\mathcal{F}$ be a coherent sheaf over X which is moreover S-flat. Then there exists a finite complex $K^\bullet = [K^0 \to \cdots \to K^n]$ of finite projective A-modules and, for all $p \geqslant 0$, an isomorphism of functors*

$$H^p(X \times_S (-), \mathcal{F} \otimes_A (-)) \simeq H^p(K^\bullet \otimes_A (-))$$

over the category of A-algebras.

Proof. The scheme X being quasi-compact, we can choose $\mathcal{U} = (U_i)_{i \in I}$ a covering of X by affine open subschemes. Let $C^\bullet = C^\bullet(\mathcal{U}, \mathcal{F})$ the alternated Čech complex of $\mathcal{U}$ with coefficients in $\mathcal{F}$. As X is separated, it is a complex of flat A-modules with degrees concentrated in $[0, \operatorname{Card} I]$. Moreover for each B-algebra, the complex

$$C^\bullet \otimes_A B = C^\bullet((U_i \times_{\operatorname{Spec} A} \operatorname{Spec} B)_{i \in I}, \mathcal{F} \otimes_A B)$$

computes the cohomology of the pull back of $\mathcal{F}$ over $X \times_{\operatorname{Spec} A} \operatorname{Spec} B$. The result is then the consequence of the following results of homological algebra :

Lemma 4.19. *Let A be a noetherian ring. Let $C^\bullet$ be a complex of A-modules concentrated in degrees $[0, n]$ and such that $H^i(C^\bullet)$ is of finite over A for $0 \leqslant i \leqslant n$. Then there exists a complex $K^\bullet = [K^0 \to \cdots \to K^n]$ of A-modules such that K^i is finite free if $i \geqslant 1$ and a quasi-isomorphism $K^\bullet \to C^\bullet$. Moreover if all the A-modules C^p are flat, then K^0 is a finite projective A-module.*

Proof. We construct by decreasing induction on m a complex $[K^m \to \cdots \to K^n]$ of finite free A-modules and a morphism of complexes

$$\begin{array}{ccccccc} K^m & \xrightarrow{d^m} & K^{m+1} & \xrightarrow{d^{m+1}} & \cdots & \xrightarrow{d^{n-1}} & K^n \\ \downarrow{\scriptstyle f^m} & & \downarrow{\scriptstyle f^{m+1}} & & & & \downarrow{\scriptstyle f^n} \\ C^m & \xrightarrow{\partial^m} & C^{m+1} & \xrightarrow{\partial^{m+1}} & \cdots & \xrightarrow{\partial^{n-1}} & C^n \end{array}$$

such that the induced maps $H^k(K^\bullet) \xrightarrow{\sim} H^k(C^\bullet)$ are isomorphisms for $m + 1 \leqslant k \leqslant n$ and surjection for $k = m$. For the case $m = n$, we choose for K^n a finite free A-module and a surjective A-modules homomorphism $K^n \twoheadrightarrow H^n(C^\bullet)$. By the freeness of K^n, this map can be lifted into a map $f^n : K^n \to C^n$. Assuming that the construction

is done for the rank $m \geqslant 1$. We choose a finite free A-module K_1^{m-1} and a map $g^{m-1} : K_1^{m-1} \to \operatorname{Ker} \partial^{m-1}$ inducing a surjection on $H^{m-1}(C^\bullet)$ and we choose an other finite free A-module K_2^{m-1} and a surjective map $K_2^{m-1} \twoheadrightarrow (f^m)^{-1}(\operatorname{Im} \partial^{m-1})$. This map can be lifted into a map $h^{m-1} : K_2^{m-1} \to C^{m-1}$. We define $K^{m-1} \coloneqq K_1^{m-1} \oplus K_2^{m-1}$ and $f^{m-1} = (g^{m-1}, h^{m-1})$. At the last step, we replace K^0 by $K^0/(\operatorname{Ker} f^0 \cap \operatorname{Ker} d^0)$.

Finally we have to prove that K^0 is finite projective when all the C^p are flat. Let $L^\bullet$ be the cone of the morphism of complexes $K^\bullet \to C^\bullet$ so that we have a long exact sequence of complexes of A-modules

$$\cdots \to H^i(K^\bullet) \to H^i(C^\bullet) \to H^i(L^\bullet) \to H^{i+1}(K^\bullet) \to \cdots .$$

The complex $(L^\bullet, D^\bullet)$ is acyclic. Moreover L^i is flat except perhaps if $i = -1$. We deduce from the flatness and acyclicity of $L^\bullet$ that the A-modules $\operatorname{Im} D^i$ are all flat for $i \geqslant 0$. We obtain a short exact sequence of A-modules

$$0 \to L^{-1} \to L^0 \to \operatorname{Im} D^0$$

with L^0 and $\operatorname{Im} D^0$ so that $L^{-1} = K^0$ is a flat A-module. Now a flat module of finite type is projective. □

Lemma 4.20. *Let $f : K^\bullet \to C^\bullet$ be some quasi-isomorphism of finite complexes of flat A-modules. Then, for all A-algebra B, the morphism*

$$K^\bullet \otimes_A B \to C^\bullet \otimes_A B$$

is a quasi-isomorphism.

Proof. Let $(L^\bullet, D^\bullet)$ be the cone of f. The complex $L^\bullet$ is finite and acyclic complex of flat A-modules. Consequently all the A-modules $\operatorname{Ker} D^i = \operatorname{Im} D^{i-1}$ are flat. This implies that the complex $L^\bullet \otimes_A B$ is acyclic. As $L^\bullet \otimes_A B$ is the cone of the map $K^\bullet \otimes_A B \to C^\bullet$, we deduce that the map $K^\bullet \otimes_A B \to C^\bullet \otimes_A B$ is a quasi-isomorphism. □

□

Corollary 4.21. *Let $f : X \to S$ be a proper map between locally noetherian schemes. Let $\mathcal{F}$ be some coherent sheaf over X which is S-flat. Then, for all $p \geqslant 0$, the map $s \mapsto \dim_{k(s)} H^p(f^{-1}(s), \mathcal{F} \mid_{f^{-1}(s)})$ is upper semi-continuous and the map $s \mapsto \chi_s(\mathcal{F}) = \sum_{p \geqslant 0} (-1)^p \dim_{k(s)} H^p(f^{-1}(s), \mathcal{F} \mid_{f^{-1}(s)})$ is locally constant.*

Proof. The problem is local on S so that we can assume that $S = \operatorname{Spec} A$ is affine. Let $K^\bullet$ be a complex obtained by Proposition 4.18. For $s \in S$, we have

$$\chi_s(\mathcal{F}) = \sum_{p \geqslant 0} (-1)^p \dim_{k(s)} K^p \otimes_A k(s).$$

The A-modules K^p are projective of finite type so that the function $s \mapsto \chi_s(\mathcal{F})$ is locally constant. On the other hand, we have

$$\dim_{k(s)} H^p(f^{-1}(s), \mathcal{F}\mid_{f^{-1}(s)}) = \dim_{k(s)} K^p \otimes_A k(s) - \operatorname{rk}(d^p \otimes \mathrm{Id}_{k(s)}) - \operatorname{rk}(d^{p-1} \otimes \mathrm{Id}_{k(s)}).$$

Consequently it is sufficient to prove that the maps $s \mapsto \operatorname{rk} d^k \otimes \mathrm{Id}_{k(s)}$ are lower semi-continuous on S. That is a consequence of the following statement

$$\operatorname{rk} d^k \otimes \mathrm{Id}_{k(s)} < r \Leftrightarrow \Lambda^r(d^k \otimes \mathrm{Id}_{k(s)}) = 0. \qquad \square$$

Let $f : X \to S$ be a morphism of schemes and let $\mathcal{F}$ be an abelian sheaf on X. For $g : T \to S$, a morphism of schemes, we can consider the following cartesian square

$$\begin{array}{ccc} X_T & \xrightarrow{g'} & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ T & \xrightarrow{g} & S. \end{array}$$

By adjunction properties there is a functorial map $\mathcal{F} \to g'_*(g')^{-1}\mathcal{F}$. Applying f_* and taking account $f \circ g' = g \circ f'$, we deduce a functorial map $f_*\mathcal{F} \to g_* f'_*(g')^{-1}\mathcal{F}$ and, by adjunction, $(g')^{-1} f_*\mathcal{F} \to f'_*(g')^{-1}\mathcal{F}$. The two functors g^{-1} and $(g')^{-1}$ are exact and right adjoints so that they send injective objects to injective objects of the category of abelian sheaves. The formalism of derived functors gives us, for all $p \geqslant 0$, a functorial map $g^{-1}R^p f_*\mathcal{F} \to R^p f'_*(g')^{-1}\mathcal{F}$. Now assume that $\mathcal{F}$ is quasi-coherent. If we compose this map with the map $R^p f'_*(g')^{-1}\mathcal{F} \to R^p f_*(g')^*\mathcal{F}$ deduced from the canonical map $(g')^{-1} \to (g')^*$, we obtain a map $g^{-1}R^p f_*\mathcal{F} \to R^p f'_*(g')^*\mathcal{F}$ which has a canonical factorisation

$$\theta_g^p : g^* R^p f_*\mathcal{F} \to R^p f'_*(g')^*\mathcal{F}.$$

We say that $R^p f_*\mathcal{F}$ *commutes with base change* if the maps θ_g^p are isomorphisms for all g (and T).

If $s \in S$ is a point and $T = \operatorname{Spec} k(s)$ and g is the map corresponding to $s \in S$, we have $X_T = f^{-1}(s)$ and $(g')^*\mathcal{F} = \mathcal{F}|_{f^{-1}(s)}$. We write $\theta_s^p = \theta_g^p$ the map

$$\theta_s^p : R^p f_*\mathcal{F} \otimes k(s) \longrightarrow H^p(f^{-1}(s), \mathcal{F}|_{f^{-1}(s)}).$$

If $S = \operatorname{Spec} A$ is a noetherian affine scheme, if f is proper and if $K^\bullet$ is as in Proposition 4.18, we can check that $R^p f_*\mathcal{F}$ commutes with base change if and only if, for all A-algebra B, the map

$$H^p(K^\bullet) \otimes_A B \longrightarrow H^p(K^\bullet \otimes_A B)$$

is an isomorphism.

Corollary 4.22. *Let $f : X \to S$ be a map of locally noetherian schemes. Assume S reduced and connected. Let $\mathcal{F}$ be a coherent sheaf on X which is S-flat. The following assertions are equivalent :*

(i) the map $s \mapsto \dim_{k(s)} H^p(f^{-1}(s), \mathcal{F}\mid_{f^{-1}(s)})$ *is constant ;*

(ii) the sheaf $R^p f_*(\mathcal{F})$ *is locally free and for all* $s \in S$*, the canonical map*

$$R^p f_*(\mathcal{F}) \otimes k(s) \xrightarrow{\sim} H^p(f^{-1}(s), \mathcal{F}\mid_{f^{-1}(s)})$$

is an isomorphism.

Moreover, under these conditions, both $R^p f_*(\mathcal{F})$ *and* $R^{p-1} f_*(\mathcal{F})$ *commutes to base change, which means that for all* $g : T \to S$*, and* $i \in \{p-1, p\}$*, we have*

$$g^* R^i f_*(\mathcal{F}) \xrightarrow{\sim} R^i f'_*((g')^*\mathcal{F}),$$

where f' *and* g' *are defined in the following cartesian diagram*

$$\begin{array}{ccc} X \times_S T & \xrightarrow{g'} & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ T & \xrightarrow{g} & S. \end{array}$$

Proof. The implication $(ii) \Rightarrow (i)$ is clear. We prove $(i) \Rightarrow (ii)$. Assume that the map $s \mapsto \dim_{k(s)} H^p(f^{-1}(s), \mathcal{F}\mid_{f^{-1}(s)})$ is constant. The statement is local on S so that we can assume that $S = \operatorname{Spec} A$ and consider a complex $K^\bullet$ obtained from Proposition 4.18. We will use several times the following lemma :

Lemma 4.23. *Let* A *be a reduced noetherian ring. If* M *is an* A*-module of finite type such that the map from* $\operatorname{Spec} A$ *to* $\mathbb{Z}$ *sending* $\mathfrak{p}$ *to* $\dim_{k(\mathfrak{p})} M \otimes_A k(\mathfrak{p})$ *is locally constant, then* M *is projective.*

Proof. Fix $\mathfrak{p} \in \operatorname{Spec} A$ and let $n = \dim_{k(\mathfrak{p})} M \otimes_A k(\mathfrak{p})$. Let $f : A^n \to M$ a morphism of A-modules inducing an isomorphism $k(\mathfrak{p})^n \xrightarrow{\sim} M \otimes_A k(\mathfrak{p})$. It follows from Nakayama Lemma that this map induces a surjection $f_\mathfrak{p} : A^n_\mathfrak{p} \twoheadrightarrow M_\mathfrak{p}$. As M is of finite type, there exists an open neighbourhood U of $\mathfrak{p}$ in $\operatorname{Spec} A$ such that, for all $\mathfrak{q} \in U$, the map $f_\mathfrak{q}$ is surjective. Consequently up to localizing A, we can assume that $f_\mathfrak{q}$ is surjective and that $\dim_{k(\mathfrak{q})} M \otimes_A k(\mathfrak{q}) = n$ for all $\mathfrak{q} \in \operatorname{Spec} A$. Consequently, if $N = \operatorname{Ker} f$, we have $N \subset \mathfrak{q} A^n$ for all $\mathfrak{q} \in \operatorname{Spec} A$. As A is reduced, this implies that $N = 0$. □

From our assumption we can deduce that the ranks of $d^p \otimes \mathrm{Id}_{k(s)}$ and $d^{p-1} \otimes \mathrm{Id}_{k(s)}$ are locally constant. This implies that the A-modules $K^p / \operatorname{Im} d^{p-1}$ and $K^{p+1} / \operatorname{Im} d^p$ are projective A-modules and consequently that the submodules $\operatorname{Ker} d^p \subset K^p$ and $\operatorname{Ker} d^{p-1} \subset K^{p-1}$ are direct factors. Consequently we have a decomposition of A-modules

$$K^p = \operatorname{Im} d^{p-1} \oplus H_p \oplus L_p, \quad \operatorname{Ker} d^p = \operatorname{Im} d^{p-1} \oplus H_p.$$

This implies that

$$H^p(K^\bullet \otimes_A B) \simeq H_p \otimes_A B \simeq H^p(K^\bullet) \otimes_A B.$$

Moreover we have a decomposition

$$K^{p-1} = \operatorname{Ker} d^{p-1} \oplus L_{p-1}$$

so that

$$H^{p-1}(K^\bullet \otimes_A B) \simeq \operatorname{Ker}(d^{p-1}) \otimes_A B / \operatorname{Im}(d^{p-1} \otimes \operatorname{Id}_B) = H^{p-1}(K^\bullet) \otimes_A B$$

since by right exactness of the tensor product, $\operatorname{Im}(d^{p-2} \otimes \operatorname{Id}_B) \simeq \operatorname{Im}(d^{p-2}) \otimes_A B$. □

Theorem 4.24. *Let $f : X \to S$ be a proper morphism between locally noetherian schemes. Let $\mathcal{F}$ be a coherent sheaf over X which is S-flat. Let $p \geqslant 0$ and let $s \in S$ be a point such that the base change map $\theta_s^p : (R^p f_* \mathcal{F}) \otimes k(s) \to H^p(f^{-1}(s), \mathcal{F}|_{f^{-1}(s)})$ is surjective. Then there exists an open neighbourhood U of s such that $R^p f_* \mathcal{F}$ commutes with base change over U. As a consequence, $\theta_{s'}^p$ is an isomorphism for all $s' \in S$. Moreover the following conditions are equivalent*

(i) the sheaf $R^p f_* \mathcal{F}$ is locally free on U ;

(ii) for all $s' \in U$, the map $\theta_{s'}^{p-1}$ is surjective.

Proof. The assertion is local on S so that we can assume that $S = \operatorname{Spec} A$ for a noetherian ring A. Let $K^\bullet$ be a perfect complex of A-modules computing $R^\bullet f_* \mathcal{F}$. Let $Z^p = \operatorname{Ker} d^p$, $B^p = \operatorname{Im} d^{p-1}$, $H^p = Z^p / B^p$ and $Z^p(s) = \operatorname{Ker} d^p \otimes \operatorname{Id}_{k(s)}$ and $B^p(s) = \operatorname{Im} d^{p-1} \otimes \operatorname{Id}_{k(s)}$. For all $p \geqslant 0$, the map $B^p \otimes k(s) \to B^p(s)$ is surjective, so that the surjectivity of $H^p \otimes k(s) \to Z^p(s)/B^p(s)$ is equivalent to the surjectivity of $Z^p \to Z^p(s)$. Up to localizing A, we can assume that Z^p is a direct factor of K^p and consequently a finite projective module. This follows from the following Lemma :

Lemma 4.25. *Let A be a local noetherian ring and $f : M \to N$ a morphism of finite free A-modules. Let k be the residue field of A, if $(\operatorname{Ker} f) \otimes_A k \to \operatorname{Ker}(f \otimes_A \operatorname{Id}_k)$ is surjective, then $\operatorname{Ker} f$ is a direct summand of M.*

Proof. Let $\overline{M}_1 = \operatorname{Ker}(f \otimes_A \operatorname{Id}_k)$ and $\overline{M}_2$ a direct summand of the k-vector space $M \otimes_A k$. By assumption, we can lift a k-basis of $\overline{M}_1$ in a family of elements of $\operatorname{Ker} f$. Choosing an other lift of a basis of $\overline{M}_2$, we find two submodules M_1 and M_2 of M such that $M_1 \subset \operatorname{Ker} f$ and $M_i \otimes_A k \simeq \overline{M}_i$ for $i \in \{1, 2\}$. Using Nakayama Lemma and the fact that M is finite free, we can conclude that $M = M_1 \oplus M_2$ so that M_1 and M_2 are finite free. Using the fact that N is finite free and that $M_2 \otimes_A k \to N \otimes_A k$ is injective by definition of $\overline{M}_2$, we can conclude that the map $M_2 \to N$ is injective and that $\operatorname{Ker} f \cap M_2 = 0$. Finally $\operatorname{Ker} f = M_1$ is a direct summand of M. □

Let B be some A-algebra. Looking at the following diagram, we see that this implies that $R^p f_* \mathcal{F}$ commutes to base change over $\operatorname{Spec} A$:

$$\begin{array}{ccccccc} & & B^p \otimes_A B & \longrightarrow & Z^p \otimes_A B & \longrightarrow & H^p \otimes_A B \longrightarrow 0 \\ & & \downarrow & & \downarrow \wr & & \downarrow \\ 0 & \longrightarrow & \operatorname{Im}(d^{p-1} \otimes \mathrm{Id}_B) & \longrightarrow & \operatorname{Ker}(d^p \otimes \mathrm{Id}_B) & \longrightarrow & H^p(X_B, \mathcal{F} \otimes_A B) \longrightarrow 0. \end{array}$$

Now assume morever (i). Then B^p is a direct factor of Z^p and thus of K^p. This implies that Z^{p-1} is a direct factor of K^{p-1} and, by what preceeds, that $R^{p-1} f_* \mathcal{F}$ commutes with base change over U. This gives (ii).

Conversely we assume (ii). Let $s \in U$. The map θ_s^{p-1} is surjective, this implies as above that Z^{p-1} is locally a direct factor of K^{p-1}. Looking at the diagram

$$\begin{array}{ccccccccc} & & Z^{p-1} \otimes_A k(s) & \longrightarrow & K^{p-1} \otimes_A k(s) & \longrightarrow & B^p \otimes_A k(s) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \wr & & \downarrow & & \\ 0 & \longrightarrow & Z^{p-1}(s) & \longrightarrow & K^{p-1} \otimes_A k(s) & \longrightarrow & B^p(s) & \longrightarrow & 0 \end{array}$$

we see that the right vertical map has to be an isomorphism. Now a diagram chasing in the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Tor}_1^A(k(s), K^p/B^p) & \longrightarrow & B^p \otimes_A k(s) & \longrightarrow & K^p \otimes_A k(s) & \longrightarrow & (K^p/B^p) \otimes_A k(s) \longrightarrow 0 \\ & & & & \downarrow \wr & & \| & & \downarrow \wr \\ & & 0 & \longrightarrow & B^p(s) & \longrightarrow & K^p \otimes_A k(s) & \longrightarrow & K^p \otimes_A k(s)/B^p(s) \longrightarrow 0 \end{array}$$

shows that $\operatorname{Tor}_A^1(k(s), K^p/B^p) = 0$, the module K^p/B^p being of finite type, this implies that K^p/B^p is flat at s and that B^p is locally a direct factor of K^p and H^p is consequently flat at s. Conversely, if H^p is locally free, the A-module B^p is locally a direct factor of Z^p and K^p, which implies that Z^{p-1} is locally a direct factor of K^{p-1} which implies easily that the map $Z^{p-1} \otimes_A k(s) \to Z^{p-1}(s)$ is surjective. □

Corollary 4.26. *Let $f : X \to S$ be some proper and smooth map with geometrically connected fibers. Then the map of coherent sheaves $\mathcal{O}_S \to f_* \mathcal{O}_X$ is an isomorphism.*

Proof. The assumption is local on S, and we can reduce ourselves to the situation where S is a noetherian scheme. For each $s \in S$, we have $H^0(f^{-1}(s), \mathcal{O}_{f^{-1}(s)}) = k(s)$ since the fibers are proper and geometrically connected. This implies that the coherent sheaf $\mathcal{O}_X$ satisfy the hypotheses of Theorem 4.24 for $p = 0$. This implies that $f_* \mathcal{O}_X$ is locally free of rank 1 and the map $\mathcal{O}_S \to f_* \mathcal{O}_X$ is surjective at every point so that it is an isomorphism. □

5 Elliptic curves

5.1 Algebraic curves over a field

Divisors Let k be a field. A *curve over k* is a k-scheme which is of finite type, separated, reduced and equidimensional of dimension 1.

The *group of divisors* of C is the free abelian group generated by the closed points of C. We denote it $\mathrm{Div}(C)$ and its elements have the form $\sum_{x\in C} m_x(x)$. It is an ordered group for the relation

$$\sum_{x\in C} m_x(x) \geqslant 0 \Leftrightarrow \forall x \in \overline{C}, m_x \geqslant 0.$$

Remark 5.1. Let Z be a closed subscheme of C which is finite over k. Then the underlying space of Z is a finite set of closed points of C and Z is the disjoint union of its localizations Z_x. Each Z_x is the spectrum of local artinian $k(x)$-algebra $\Gamma(Z_x, \mathcal{O})$ and we define

$$[Z] \coloneqq \sum_{x\in Z} \lg(\Gamma(Z_x, \mathcal{O}))(x).$$

Such a divisor $[Z]$ is called an *effective divisor*.

We define a group homomorphism from $\mathrm{Div}(C)$ to $\mathbb{Z}$, called *degree*, by the formula $\deg(x) = [k(x) : k]$. The kernel of deg is denoted $\mathrm{Div}^0(C) \subset \mathrm{Div}(C)$.

Remark 5.2. It $[Z]$ is an effective divisor of C, we have $\deg([Z]) = \dim_k \Gamma(Z, \mathcal{O})$.

Principal divisors and class group From now on we will assume that C is smooth over k and irreducible (or equivalently connected).

For $x \in C$ a closed point, the local ring $\mathcal{O}_{C,x}$ is a discrete valuation ring. Let v_x be its valuation that we extend to the fraction field $k(C)$. If $f \in k(C)^\times$, the *divisor of f* is defined by $\mathrm{div}(f) \coloneqq \sum_{x\in C} v_x(f)(x)$. Since all the v_x are valuation, the map div induces a group homomorphism from $k(C)^\times$ to $\mathrm{Div}(C)$. We say that two divisors D_1 and D_2 of C are *linearly equivalent*, and we note it $D_1 \sim D_2$, if their difference is in the image of div. We define $\mathrm{Cl}(C) \coloneqq \mathrm{Div}(C)/\mathrm{div}(k(C)^\times)$ the group of linear equivalence classes. Clearly two smooth irreducible curves which are isomorphic have isomorphic groups of divisors.

Example 5.3. If $C = \mathbb{A}^1_k$, then $\mathrm{Cl}(C) = 0$.

The case of proper and smooth curves Let C be a proper, smooth and irreducible curve. In this case, for $f \in k(C)^\times$, we have

$$\deg(\mathrm{div}\, f) = 0.$$

As a consequence the subgroup of principal divisors is contained in $\mathrm{Div}^0(C)$ and the degree map factors through $\mathrm{Cl}(C)$. Let $\mathrm{Cl}^0(C)$ be its kernel which identifies to the quotient $\mathrm{Div}^0(C)/\operatorname{div}(k(C)^\times)$.

Example 5.4. If $C = \mathbb{P}^1_k$, we have $\mathrm{Cl}^0(C) = 0$ and deg induces an isomorphism $\mathrm{Cl}(C) \simeq \mathbb{Z}$.

Invertible sheaves and divisors Let C be a smooth and irreducible curve over k.

Let $x \in C$ be a closed point. As C is a regular scheme of dimension 1, the sheaf $\mathcal{I}(x) \coloneqq \mathrm{Ker}(\mathcal{O}_C \to k(x))$ is a locally principal ideal of $\mathcal{O}_C$. Let $\mathcal{L}(x) \coloneqq \mathcal{H}om(\mathcal{I}(x), \mathcal{O}_C)$ be its dual. If $D = \sum_x m_x(x) \in \mathrm{Div}(X)$ is a divisor, we can construct two invertible sheaves

$$\mathcal{I}(D) \coloneqq \bigotimes_{x \in C} \mathcal{I}(x)^{\otimes m_x}, \quad \mathcal{L}(D) \coloneqq \mathcal{I}(D)^{-1}.$$

Let $\mathcal{K}_C$ be the sheaf associated to the presheaf $U \mapsto \operatorname{Frac} \Gamma(U, \mathcal{O}_C)$ on C. It is the constant sheaf associated to the k-algebra $k(C)$.

If $\mathcal{L}$ is an invertible subsheaf of $\mathcal{K}_C$, there is a canonical isomorphism of invertible sheaves between $\mathcal{L}^{-1}$ and the subsheaf of $\mathcal{K}$ defined by $\{a \in \mathcal{K},\, a\mathcal{L} \subset \mathcal{O}\}$. This isomorphism is compatible with the tensor product and is involutive, so that we can canonically identify each invertible sheaf $\mathcal{L}(D)$ to a subsheaf of $\mathcal{K}$. The map $D \mapsto \mathcal{L}(D)$ induces actually a bijection between $\mathrm{Div}(C)$ and the set of invertible subsheaves of $\mathcal{K}_C$. If $U = \operatorname{Spec} A$ is an affine open subset of C, then the space of sections of the sheaf $\mathcal{L}(D)$ on U is

$$H^0(U, \mathcal{L}(D)) = \{f \in k(C) \mid \operatorname{div}(f|_U) + D|_U \geqslant 0\}.$$

It is now clear that a divisor D is principal if and only if the sheaf $\mathcal{L}(D)$ is isomorphic to $\mathcal{O}_C$.

Lemma 5.5. *Let $\mathcal{F}$ be a coherent sheaf of $\mathcal{K}_C$-modules. Then there exists $n \in \mathbb{N}$ such that $\mathcal{F} \simeq \mathcal{K}_C^n$.*

Proof. Let j be the inclusion of the generic point η of C in C. The canonical map of sheaves $a : \mathcal{F} \to j_* j^* \mathcal{F}$ is an isomorphism. Namely it is sufficient to be checked sufficiently small non empty open subsets of C. Consequently we can assume that $\mathcal{F}$ is generated by its global sections on some non empty open subset $U \subset C$. Tthe space of these global sections of $\mathcal{F}$ over U is a finite dimensional $k(C)$-vector space. Consequently it is a free $\mathcal{K}_U$-module for which it is easy to check that a is an isomorphism. □

From Lemma 5.5 we conclude that if $\mathcal{L}$ is an invertible sheaf on C, then there exists an isomorphism $\mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{K} \simeq \mathcal{K}$. This shows that every invertible sheaf on C is isomorphic to a subsheaf of $\mathcal{K}$. From this analysis we can conclude that the map $D \mapsto \mathcal{L}(D)$ induces an isomorphism of groups

$$\mathrm{Cl}(C) \xrightarrow{\sim} \mathrm{Pic}(C).$$

Using this isomorphism we can define the *degree* of an invertible sheaf $\mathcal{L}$ as the degree of a divisor D such that $\mathcal{L} \simeq \mathcal{L}(D)$.

The Riemann-Roch theorem Let C be an irreducible proper and smooth curve over k. We define the *genus* of C as being the integer $g(C) \coloneqq \dim_k H^1(C, \mathcal{O}_C)$.

Theorem 5.6. *Let $\mathcal{L}$ be an invertible sheaf on C.*

(i) If $H^0(C, \mathcal{L}) \neq 0$, then $\deg \mathcal{L} \geqslant 0$.

(ii) We have an equality of dimensions

$$\dim_k H^0(C, \mathcal{L}) - \dim_k H^1(C, \mathcal{L}) = \deg \mathcal{L} + 1 - g.$$

(iii) There is an isomorphism of k-vector spaces between $H^1(C, \mathcal{L})$ and $H^0(C, \mathcal{L}^{-1} \otimes_{\mathcal{O}_C} \Omega^1_{C/k})$.

Corollary 5.7. *We have $\deg \Omega^1_{C/k} = 2(g-1)$. Moreover, if $\deg \mathcal{L} > 2(g-1)$, then $H^1(C, \mathcal{L}) = 0$ and*

$$\dim_k H^0(C, \mathcal{L}) = 1 - g + \deg \mathcal{L}.$$

Proof. We compute $\deg \Omega^1_{C/k}$ by applying theorem 5.6 to the invertible sheaf $\mathcal{L} = \Omega^1_{C/k}$. Moreover if $\deg \mathcal{L} > 2(g-1)$ then, $\deg(\mathcal{L}^{-1} \otimes_{\mathcal{O}_C} \Omega^1_{C/k}) < 0$ and

$$H^1(C, \mathcal{L}) = H^0(C, \mathcal{L}^{-1} \otimes_{\mathcal{O}_C} \Omega^1_{C/k}) = 0. \qquad \square$$

We will use the following other consequence of the Riemann-Roch Theorem (see [Har77, Cor. IV.3.2]):

Theorem 5.8. *Let C be a proper smooth and geometrically connected curve over k. If $\deg \mathcal{L} \geqslant 2g(C) + 1$, the sheaf $\mathcal{L}$ is very ample. This implies that the canonical map*

$$C \to \mathbb{P}(H^0(C, \mathcal{L}))$$

sending a point x to the kernel of $H^0(C, \mathcal{L}) \to H^0(x, \mathcal{L}|_{\{x\}})$ is well defined (the kernel is an hyperplane) and is a closed embedding.

5.2 Elliptic curves over a field

Let k be a field. An *elliptic curve* over k is a pair $(E, 0)$ where E is a proper smooth connected curve over k of genus 1 and $0 \in E(k)$. If $(E, 0)$ is an elliptic curve and K/k is an extension, then E_K is a regular scheme, so that the connected components of E_K coincide with its irreducible components. Moreover E having a k-rational point, we conclude that E is automatically geometrically irreducible.

Group law on an elliptic curve

Theorem 5.9 (Abel-Jacobi Theorem)**.** *Let $(E,0)$ be an elliptic curve over k. Then the map $P \mapsto [P]-[0]$ induces a bijection from $E(k)$ to $\mathrm{Cl}^0(E)$.*

Proof. Assume that $[P]-[0] \sim [Q]-[0]$, then there exists $f \in k(E)^\times$ such that $[P]-[Q] = \mathrm{div}(f)$. We have $\deg \mathcal{L}(Q) = 1$ so that by Corollary 5.7 the space $H^0(C, \mathcal{L}(Q))$ has dimension one and coincides with the space of constant functions. As f is an element of this space, $f \in k^\times$ and $\mathrm{div}(f) = 0$. This implies $P = Q$.

Let $D \in \mathrm{Div}^0(E)$. Corollary 5.7 implies that $\dim H^0(C, \mathcal{L}(D+(0))) = 1$. Let f be a non zero element of this space. By definition

$$\mathrm{div}(f) + D + (0) \geqslant 0.$$

As a positive divisor of degree 1 is necessarily of the form (P) for some $P \in E(k)$, there exists a point $P \in E(k)$ such that $\mathrm{div}(f) + D + (0) = (P)$, hence $D \sim (P) - (0)$. □

Using the Abel-Jacobi map we define a group law on the set $E(k)$, that is for $(P,Q) \in E(k)^2$, the point $P+Q$ is the unique element of $E(k)$ such that

$$(P+Q) + (0) \sim (P) + (Q).$$

It follows from Theorem 5.9 that $(E(k), +)$ is an abelian group with neutral element 0.

Weierstrass equations Let $(E,0)$ be an elliptic curve over k. Then there exists a closed embedding $E \hookrightarrow \mathbb{P}(H^0(E, \mathcal{L}(3(0)))) \simeq \mathbb{P}^2_k$. Giving an explicit form to this embedding leads us to the notion of *Weierstrass equation*.

By Corollary 5.7, for $n \geqslant 1$, the k-vector space $H^0(E, \mathcal{O}_E(n(0)))$ has dimension n. Consequently there exists elements x and y in $k(E)$ such that $(1,x)$ is a basis of $H^0(E, \mathcal{O}_E(2(0)))$ and $(1,x,y)$ is a basis of $H^0(E, \mathcal{L}(3(0)))$. Actually the rational functions x and y are defined over $E \smallsetminus \{0\}$ and satisfy $v_0(x) = -2$, $v_0(y) = -3$. Therefore $(1,x,y,x^2)$ is a basis of $H^0(E, \mathcal{L}(4(0)))$ and $(1,x,y,x^2,xy)$ is a basis of $H^0(E, \mathcal{L}(5(0)))$. Finally as $v_0(x^3) = v_0(y^2) = -6$, there exists $(a_1,a_2,a_3,a_4,a_6,\alpha) \in k^5 \times k^\times$ such that

$$y^2 + a_1xy + a_3y = \alpha x^3 + a_2x^2 + a_4x + a_6.$$

Replacing x and y by non zero scalar multiples, we can assume that $\alpha = 1$. Then the rational function x and y satisfy a so called *Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4}$$

Equation (4) is clearly an irreducible polynomial in $k[x,y]$. Therefore the closure in $\mathbb{P}^2_k$ of its vanishing locus is an irreducible algebraic curve. Using Theorem 5.8 applied to

$\mathcal{L}(0)^{\otimes 3}$, we construct an embedding of E into $\mathbb{P}^2(k)$ which lies in this algebraic curve and gives an isomorphic. In other words $E \smallsetminus \{0\}$ is an affine curve isomorphic to

$$\operatorname{Spec} k[x,y]/(y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)).$$

Conversely consider an equation of the form (4). Let E be the closure in $\mathbb{P}^2_k$ of its vanishing locus. Then E is an irreducible algebraic curve over k. It has a unique point "at the infinity". Call it 0. Then E is smooth over k if and only if the affine curve $E \smallsetminus \{0\}$ is smooth over k.

Conversely it can be directly checked that, given some affine smooth Weierstrass equation (4), then its schematic closure in $\mathbb{P}^2_k$ is a proper and smooth algebraic curve of genus 1. As its infinite point is k-rational, we obtain an elliptic curve. We can also use the adjonction formula stating that a closed smooth curve in $\mathbb{P}^2_k$ defined by an equation of degree d has genus $\frac{d(d-3)}{2} + 1$. This is a consequence of Bezout Theorem and the classification of invertible sheaves on $\mathbb{P}^2_k$.

5.3 Elliptic curves over an arbitrary base

Let S be a scheme. A *curve* over S is map of schemes $f : C \to S$ which is separated, flat of finite presentation with all its fibers equidimensional of dimension 1. A curve $f : C \to S$ is *proper* is f is proper and *smooth* if f is smooth. From the flatness of f, we know that the map from S to $\mathbb{Z}$ defined by $s \mapsto 1 - \chi_s(\mathcal{O}_C)$ is locally constant. This locally constant map is called the *genus* of $f : C \to S$.

Let $\mathcal{L}$ be an invertible sheaf over C. By the flatness of f, the map $s \mapsto \chi_s(\mathcal{L})$ is locally constant on S. By Theorem 5.6 so is the map $\deg \mathcal{L} : s \mapsto \deg \mathcal{L}|_{f^{-1}(s)}$ which is called the *degree* of $\mathcal{L}$.

An *elliptic curve* over S is a pair $(E, 0)$ where E is proper and smooth curve over S of genus 1 with connected fibers and $0 \in E(S)$ is a section of $f : E \to S$. The existence of a section and the smoothness of E/S implies that the geometric fibers of E/S are irreducible. As a consequence the structural map $\mathcal{O}_S \to f\mathcal{O}_E$ is an isomorphism.

Abel-Jacobi Theorem for elliptic curves over S Let E/S be an elliptic curve. The *relative Picard group* of E/S is defined the cokernel $\operatorname{Pic}(E/S)$ of the group homomorphism $f^* : \operatorname{Pic}(S) \to \operatorname{Pic}(E)$. Using the section 0, we can define a group homomorphism $0^* : \operatorname{Pic}(E) \to \operatorname{Pic}(S)$. As 0 is a section of f, the map f^* is injective and $\operatorname{Pic}(S)$ is identified to a subgroup of $\operatorname{Pic}(E)$.

As 0 is a section of f, the composition of the inclusion $\operatorname{Ker} 0^*$ into $\operatorname{Pic}(E)$ with the quotient map is an isomorphism $\operatorname{Ker} 0^* \xrightarrow{\sim} \operatorname{Pic}(E/S)$ so that we can identify $\operatorname{Pic}(E/S)$ to a subgroup of $\operatorname{Pic}(E)$.

Let $\operatorname{Pic}(E)^0$ the kernel of the degree map. The image of f^* is clearly contained in $\operatorname{Pic}(E)^0$ so that the degree map factors through $\operatorname{Pic}(E/S)$ and we define $\operatorname{Pic}(E/S)^0 \subset$

$\mathrm{Pic}(E/S)$ as the kernel of this degree map. Now consider $P \in E(S)$ a section. We use the same symbol to denote its schematic image which is a closed subscheme of E isomorphic to S. The annihilator $\mathcal{I}(P)$ of this closed subscheme is a locally principal ideal of $\mathcal{O}_E$ and we define the invertible sheaf $\mathcal{L}(P)$ as $\mathcal{I}(P)^{-1}$. Using the case of an elliptic curve over a field, we check that $\deg \mathcal{L}(P) = 1$.

Theorem 5.10. *The map $P \mapsto \mathcal{L}(P) \otimes_{\mathcal{O}_E} \mathcal{L}(0)^{-1}$ induces a bijection from $E(S)$ to $\mathrm{Pic}(E/S)^0$.*

Proof. First of all, let us remark that the functor $U \mapsto E(U)$ is a sheaf for the Zariski topology on S. As a first step, we prove that the functor $\mapsto \mathrm{Ker}(0^* : \mathrm{Pic}(E_U) \to \mathrm{Pic}(U))$ is also a sheaf for the Zariski topology on S.

Lemma 5.11. *The functor $\mapsto \mathrm{Ker}(0^* : \mathrm{Pic}(E_U) \to \mathrm{Pic}(U))$ is a sheaf for the Zariski topology on S.*

Proof. Let $(U_i)_{i\in I}$ be some open covering of S. For each $i \in I$ let $\mathcal{L}_i$ be some invertible sheaf on E_{U_i}. We assume that these data satisfy $0^*\mathcal{L}_i \simeq \mathcal{O}_{U_i}$ and $\mathcal{L}_i|_{U_{i,j}} \simeq \mathcal{L}_j|_{U_{i,j}}$ on $U_{i,j} = U_i \cap U_j$. We have to check that there exists a family of isomorphisms

$$\alpha_{i,j} : \mathcal{L}_i|_{U_{i,j}} \simeq \mathcal{L}_j|_{U_{i,j}}$$

such that

$$\forall (i,j,k) \in I^3, \quad \alpha_{i,k}|_{U_{i,j,k}} = \alpha_{j,k}|_{U_{i,jk}} \circ \alpha_{i,j}|_{U_{i,jk}}. \tag{5}$$

Namely this is the sufficient and necessary condition for the existence of an invertible sheaf $\mathcal{L}$ on E such that $\mathcal{L}|_{E_{U_{i,j}}} \simeq \mathcal{L}_i$. We know that the set $\mathrm{Iso}(\mathcal{L}_i|_{U_{i,j}}, \mathcal{L}_j|_{U_{i,j}})$ is non empty. It is consequently in natural bijection with the group $\mathrm{Aut}(\mathcal{L}_j|_{U_{i,j}})$. As $\mathcal{L}_i$ is an invertible sheaf, we have

$$\mathrm{Aut}(\mathcal{L}_j|_{U_{i,j}}) \simeq H^0(U_{i,j} f_* \mathcal{O}_E^\times) = H^0(S, \mathcal{O}_S^\times)$$

since $f_*\mathcal{O}_E = \mathcal{O}_S$. We can deduce from these bijection that the functor 0^* induces a bijection

$$\mathrm{Iso}(\mathcal{L}_i|_{U_{i,j}}, \mathcal{L}_j|_{U_{i,j}}) \simeq \mathrm{Aut}(\mathcal{O}_S).$$

We choose $\alpha_{i,j}$ such that $0^*\alpha_{i,j} = \mathrm{Id}_{U_{i,j}}$. This choice is unique satisfies the desired compatibility (5). □

We can deduce from this lemma that the functor $U \mapsto \mathrm{Pic}(E_U/U)^0$ is a sheaf for the Zariski topology on S. This implies that it is sufficient to prove the theorem locally for the Zariski topology so that we can assume that S is affine. Both functors $A \mapsto E(\mathrm{Spec}\, A)$ and $A \mapsto \mathrm{Pic}^0(E_A/\mathrm{Spec}\, A)$ commute with inductive limits so that we can assume that $S = \mathrm{Spec}\, A$ with A a noetherian ring.

Let $\mathrm{Pic}(E/S)^{(1)} \subset \mathrm{Pic}(E/S)$ be the preimage of 1 under deg. After translation by $\mathcal{O}_E(0)$ it is equivalent to prove that the map $P \mapsto \mathcal{L}(P)$ is bijective.

Let $\mathcal{L}$ be some invertible sheaf of degree 1 over E. The fibers of f are one dimensional, so that the formation of $R^1 f_*$ commutes with base change. Applying Theorem 5.6 to geometric fibers of f, we see that $R^1 f_* \mathcal{L} = 0$ and thaf $f_* \mathcal{L}$ is an invertible sheaf of formation compatible to base change. This implies that locally $f_* \mathcal{L}$ has a section and that $H^0(\operatorname{Spec} A, f_* \mathcal{L}) \simeq A$. Let $s \in H^0(E, \mathcal{L}) \simeq H^0(\operatorname{Spec} A, f_* \mathcal{L})$ be a generator of this A-module. The section s induces an injective map of sheaves $\mathcal{O}_E \hookrightarrow \mathcal{L}$ and let Z be the schematic support of the coherent sheaf $\mathcal{L}/\mathcal{O}_E$. It is easy to check that Z does not depend on the choice of s so that we can write it $Z_{\mathcal{L}}$. As $Z_{\mathcal{L}}$ is a proper scheme of locally of finite presentation and as its fibres over S are finite, it is a finite S-scheme. We claim that the map $Z_{\mathcal{L}} \to S$ is an isomorphism so that $Z_{\mathcal{L}}$ is the image of a unique element of $E(S)$. As $\mathcal{L}$ is locally generated by an element we can, up to shrinking S, assume that $\mathcal{O}_{Z_{\mathcal{L}}} \simeq \mathcal{L}/\mathcal{O}_E$. It is sufficient thus to prove that the coherent sheaf $f_*(\mathcal{L}/\mathcal{O}_E)$ is locally isomorphic to $\mathcal{O}_S$. We use the following exact sequence of cohomology

$$0 \longrightarrow f_* \mathcal{O}_E \xrightarrow{\sim} f_* \mathcal{O}_E \xrightarrow{0} f_*(\mathcal{L}/\mathcal{O}_E) \longrightarrow R^1 f_* \mathcal{O}_E \longrightarrow R^1 f_* \mathcal{L} = 0.$$

Using Theorem 4.24, we can check that $R^1 f_* \mathcal{O}_E$ is locally free of rank 1. This is enough. Now we have a short exact sequence

$$0 \longrightarrow \mathcal{O}_E \longrightarrow \mathcal{L} \longrightarrow \mathcal{O}_{Z_{\mathcal{L}}} \longrightarrow 0.$$

If we take its tensor product with $\mathcal{L}^{-1}$, we see that $\mathcal{L}^{-1} \simeq I(Z_{\mathcal{L}})$ and $\mathcal{L} \simeq \mathcal{L}(Z_{\mathcal{L}})$. Conversely if $P \in E(S)$, the support of $\mathcal{L}(P)/\mathcal{O}_E$ contains the section P, so that $Z_{\mathcal{L}(P)} = P$. Finally the map $\mathcal{L} \mapsto Z_{\mathcal{L}}$ is reciprocal to $P \mapsto \mathcal{L}(P)$. □

The bijection $E(S) \simeq \operatorname{Pic}^0(E/S)$ is clearly functorial. Moreover for each map $S' \to S$, the induced map $\operatorname{Pic}^0(E/S) \to \operatorname{Pic}^0(E_{S'}/S')$ is a group homomorphism. This implies that the functor $S \mapsto E(S)$ is a contravariant functor from the category of S-scheme to the category of groups and that there is a natural structure of *group scheme* over E. More precisely there exists a map of schemes $E \times_S E \to E$ inducing the group structure on $E(T)$ for each S-scheme T. Moreover there exists a map of S-schemes $E \to E$ inducing the inverse on $E(T)$ for each S-scheme T and we check easily that $0 \in E(S)$ is the neutral section for this structure of S-group scheme.

Weierstrass equations for elliptic curves over a general scheme Let E/S be an elliptic curve over a scheme S. For $n \geqslant 1$, the $\mathcal{O}_S$-sheaf $f_* \mathcal{L}(0)^{\otimes n}$ is locally free of rank n. Replacing S by an affine open subscheme $\operatorname{Spec} A$, we can assume that

$$H^0(S, f_* \mathcal{L}(0)^{\otimes 2}) = A \oplus Ax, \quad H^0(S, f_* \mathcal{L}(0)^{\otimes 3}) = A \oplus Ax \oplus Ay,$$

where the embedding of $H^0(S, f_* \mathcal{L}(0)^{\otimes n})$ in $H^0(S, f_* \mathcal{L}(0)^{\otimes (n+1)})$ is induced by a global section, well defined up to an element of $A^\times$, of $H^0(S, f_* \mathcal{L}(0)) \simeq A$. The elements x and y satisfy some Weierstrass equation in $H^0(S, f_* \mathcal{L}(0)^6)$:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

for elements a_1, a_2, a_3, a_4, a_6 in A. Using Riemann-Roch theorem and [Gro61b, Prop. 2.6.1], we can prove that the sheaf $\mathcal{L}(0)$ is relatively ample. This implies ([Gro61a, Prop. 4.6.2]) that we have an immersion

$$E \hookrightarrow \mathbb{P}(H^0(\operatorname{Spec} A, f_*\mathcal{L}(0)^3))$$

whose image is contained in the locus defined by the equation

$$y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2a_6z^3.$$

As the fibers of this locus are all reduced and irreducible of dimension 1, we conclude that we must have an isomorphism

$$E \simeq \operatorname{Proj}\left(A[x,y,z]/(y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2a_6z^3)\right).$$

Let $\widetilde{S} = \operatorname{Spec} \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ and

$$\widetilde{E} \coloneqq \operatorname{Proj}_{\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]}\Big(\mathbb{Z}[a_1,a_2,a_3,a_4,a_6][x,y,z]/(y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2a_6z^3)\Big)$$

the universal Weierstrass equation over $\widetilde{S}$. We define S^{univ} as the set of points $s \in \widetilde{s}$ such that $\widetilde{E} \times_{\widetilde{S}} s$ is a smooth curve. As $\widetilde{E}$ is proper over $\widetilde{S}$, the subset S^{univ} is open in $\widetilde{S}$ and it is easy to check that it contains points of all characteristics. Let E^{univ} be the restriction of $\widetilde{E}$ to S^{univ}. The local existence of a Weierstrass equation for an elliptic curve implies the following result :

Theorem 5.12. *Let E/S be an elliptic curve. For all $s \in S$ there exists an open neighbourhood U of s in U and a map $\psi : U \to S^{\text{univ}}$ inducing an isomorphism $E \simeq U \times_{S^{\text{univ}}} E^{\text{univ}}$.*

We can use this "reduction to the universal case" to prove the following consequence of Grothendieck-Serre duality :

Corollary 5.13. *Let $f : E \to S$ be an elliptic curve. The sheaves $R^1f_*\Omega^1_{E/S}$ and $f_*\Omega^1_{E/S}$ are locally free of rank one.*

Proof. The assertion is local on S. The fibers of f being of dimension 1, we know that $R^1f_*\Omega^1_{E/S}$ commutes with base change and has stalks of rank 1 by Riemann-Roch theorem. If the base if reduced we can conclude that $R^1f_*\Omega^1_{E/S}$ is locally free. As S^{univ} is reduced, the result is true for $E^{\text{univ}} \to S^{\text{univ}}$. Consequently it is true for E/S since the formation of $R^1f_*\Omega^1_{E/S}$ commutes with base change. Consequently the sheaf $f_*\Omega^1_{E/S}$ commutes with base change and has stalks of rank 1 by Riemann-Roch Theorem. As there is no cohomology in degree -1, the sheaf is automatically locally free. □

5.4 Elliptic curves over $\mathbb{C}$

Let $\Lambda \in \mathbb{C}$ be a lattice and let $\mathfrak{p}$ be the Weierstrass function associated to this lattice. We proved the following equation

$$(\mathfrak{p}')^2 = 4\mathfrak{p}^3 - g_4(\Lambda)\mathfrak{p} - g_6(\Lambda)$$

and that the polynomial $4X^3 - g_4(\Lambda)X - g_6(\Lambda)$ is separated. This proves that the projective curve defined by the Weierstrass equation

$$Y^2Z = 4X^3 - g_4(\Lambda)XZ^2 - g_6(\Lambda)$$

is smooth and is consequently an elliptic curve that we call E_Λ (the neutral element is as usual the point $(0:1:0)$). Consequently the set $E_\Lambda(\mathbb{C})$ has a structure of a compact Riemann surface and the map

$$\Psi_\Lambda : \begin{array}{ccc} \mathcal{E}_\Lambda = \mathbb{C}/\Lambda & \longrightarrow & E_\Lambda(\mathbb{C}) \\ z & \longmapsto & (\mathfrak{p}(z) : \mathrm{p}'(z) : 1) \end{array}$$

is a morphism of compact Riemann surfaces. Using Lemma 1.2 or directly Theorem 1.3 we see that the map Ψ_Λ is an isomorphism of Riemann surfaces.

Theorem 5.14. *The map Ψ_Λ is an isomorphism of groups.*

Proof. It is enough to prove that $\Psi_\Lambda(P) + \Psi_\Lambda(Q) = 0 \Leftrightarrow P + Q = 0$ and $\Psi_\Lambda(P) + \Psi_\Lambda(Q) + \Psi_\Lambda(R) = 0 \Leftrightarrow P + Q + R = 0$. The two cases are similar, let's do the second one. Saying that $\Psi_\Lambda(P) + \Psi_\Lambda(Q) + \Psi_\Lambda(R) = 0$ means that there exists some rational function $f \in k(E_\Lambda) \simeq \mathbb{C}(X)[Y]/(Y^2 - 4X^3 + g_4(\Lambda)X + g_6(\Lambda))$ on E_Λ whose divisor is $(\Psi_\Lambda(P)) + (\Psi_\Lambda(Q)) + (\Psi_\Lambda(R)) - 3(0)$. This implies that the elliptic function $f(\mathfrak{p}, \mathfrak{p}')$ on $\mathcal{E}_\Lambda$ has divisor $(P) + (Q) + (R) - 3(0)$. The conclusion follows from formulas (1). □

Theorem 5.15. *If $(E, 0)$ is an elliptic curve defined over $\mathbb{C}$, then there is a lattice Λ such that $(E, 0) \simeq (E_\Lambda, (0:1:0))$.*

Proof. We know that E is defined by a Weierstrass equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Via a well chosen change of variable we can assume that E is defined by the equation

$$y^2z = 4x^3 - Ax - B.$$

We can consider the quantity $j = \frac{1728A^3}{A^3 - 27B^2}$. It follows from Corollary 1.12 that there exists a lattice $\tau \in \mathbb{C}$ such that $j(\tau) = j$, ie

$$\frac{1728g_4(\tau)^3}{g_4(\tau)^3 - 27g_6(\tau)^2} = \frac{1728A^3}{A^3 - 27B^2}.$$

We deduce from this equality that there exists $c \in \mathbb{C}^\times$ such that $A = c^4g_4(\tau) = g_4(c^{-1}\Lambda_\tau)$ and $B = c^6g_6(\tau) = g_6(c^{-1}\Lambda_\tau)$. This implies that $E \simeq E_{c^{-1}\Lambda} \simeq E_\Lambda$. □

Corollary 5.16. *Let E be some elliptic curve defined over $\mathbb{C}$. Then, for $N \geqslant 1$, the N-torsion subgroup of $E[N](\mathbb{C})$ of $E(\mathbb{C})$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2.*

Proof. This is a direct consequence of Theorems 5.15 and 5.14. Namely there exists a lattice $\Lambda \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ as a group and

$$(\mathbb{C}/\Lambda)[N] = N^{-1}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

□

5.5 The multiplication $[N]$

Let E and E' be two elliptic curves on S. An *isogeny* from E to E' is a morphism of group schemes from E to E' which is non constant on each connected component of S. If $S = \operatorname{Spec} k$ for k a field, it is simply a non constant group schemes homomorphism.

The Lie algebra (see [DG70, §II.3]) Let S be a scheme. We define $S[\varepsilon]$ as the finite locally free S-scheme corresponding to the coherent S-algebra $\mathcal{O}_S[X]/(X^2)$. If X is an S-scheme, the *tangent bundle* $T_{X/S}$ of X/S is the S-scheme representing the functor $\mathcal{H}om_S(S[\varepsilon], X)$. If $u \in X(S)$ is a section, the *tangent space* of X/S at u is the pullback of $T_{X/S}$ along u. When G is an S-group scheme, the *Lie algebra* $\operatorname{Lie}(G/S)$ of G/S is the tangent space of G/S at the neutral section. We have canonical isomorphism $T_{G/S} \simeq \mathbb{V}(\Omega^1_{G/S})$ and $\operatorname{Lie}(G/S) \simeq \mathbb{V}(e^*\Omega^1_{G/S})$ so that if G/S is smooth, the S-scheme $\operatorname{Lie}(G/S)$ can be identify to a vector bundle over S.

The scheme $\operatorname{Lie}(G/S)$ has a natural structure of scheme in $\mathcal{O}_S$-modules. However it has a second group structure coming from the structure of group scheme over G. Namely, for each open subset $U \subset S$, we have

$$\operatorname{Lie}(G/S)(U) = \operatorname{Ker}(G(S[\varepsilon]) \to G(S)).$$

It follows from [DG70, Cor. 3.9.3, 3.5.1] that these two group laws coincide. In particular we can deduce that if G/S is a group scheme, then, for $N \in \mathbb{N}^*$, the map $[N]$ of multiplication by N in G induces a map $\operatorname{Lie}(G/S) \xrightarrow{[N]} \operatorname{Lie}(G/S)$ which coincides with the multiplication by $N \in \mathcal{O}_S$. Equivalently :

Corollary 5.17. *Let G/S be a group scheme and let $N \in \mathbb{N}^*$, then the map of $\mathcal{O}_S$-modules $[N]^* : e^*\Omega^1_{G/S} \to e^*\Omega^1_{G/S}$ coincide with the multiplication by $N \in \mathcal{O}_S$.*

Corollary 5.18. *If $f : G \to S$ is a smooth group scheme of finite presentation and if $N \in \Gamma(S, \mathcal{O}_S)^\times$, then the map of S-schemes $[N] : G \to G$ is étale.*

Proof. As G/S is smooth, we have to show that, for $x \in G$, the map $[N]$ induces an isomorphism from $\Omega^1_{G/S} \otimes k([N]x)$ to $\Omega^1_{G/S} \otimes k(x)$. We can work in the fibre over

$f(x)$ and consequently we are reduce to the case where S is $\operatorname{Spec} k$ for k a field. As $\Omega^1_{G/k} \otimes k' \simeq \Omega^1_{G_{k'}/k'}$ for k' an extension of k, we can assume that $k = k(x)$. As $y \mapsto xy$ induces an automorphism of G/k, we can even assume that x is the neutral element. It is then a consequence of Corollary 5.17. □

Multiplication Flatness is often a delicate notion to prove. We will use the following two criterions.

Theorem 5.19. *Let $f : X \to Y$ be a quasi-finite map between two regular schemes of the same dimension. Then f is flat.*

Proof. This is a local statement. We are consequently reduced to prove that if A and B are two noetherian local regular rings and $f : A \to B$ is a local map such that $B/\mathfrak{m}_A B$ is a finite dimensional k_A-vector space, then B is a flat A-module. It is [Gro64, Cor. 17.3.5.(ii)] but we can sketch a proof.

Let $(x_1, \dots, x_d)$ be a regular sequence generating $\mathfrak{m}_A$, then $(f(x_1), \dots, f(x_d))$ is a B-regular sequence. Then we proceed inductively using the following result ([Gro64, Prop. 16.5.5]): if A is a local Cohen-Macaulay ring and $x \in \mathfrak{m}_A$, then x is A-regular if and only if A/xA is has dimension $\dim A - 1$ and then A/xA is Cohen-Macaulay. □

Theorem 5.20. *Let E/S be an elliptic curve and let $N \geqslant 1$. The map $[N]$ from E to E is finite flat of degree N^2. Moreover it is étale if and only if N is invertible over S.*

Proof. Locally on S, the curve E is obtained by pullback from the universal curve over $\operatorname{Spec} \mathbb{Z}[a_1, a_2, a_3, a_4, a_5]$. Consequently we can assume that S is an affine open subset of $\operatorname{Spec} \mathbb{Z}[a_1, a_2, a_3, a_4, a_5]$ and E is the universal curve over S. In particular S is irreducible and its generic point has characteristic 0.

In a first step, we will assume that $S = S[1/N]$ and prove that $[N]$ is finite étale of degree N^2. As E is smooth over S and $[N]$ induces an isomorphism $[N]^*\Omega^1_{E/S} \xrightarrow{\sim} \Omega^1_{E/S}$, the map $[N]$ is étale. As E/S is proper, the map $[N]$ is proper. Being quasi-finite and proper between noetherian schemes, it is automatically finite. This proves that $[N]$ is finite étale. As S is irreducible, its degree is constant. As the generic point of S is of characteristic zero, $S(\mathbb{C}) \neq \emptyset$, consequently we can choose a $\mathbb{C}$-points to compute its degree which consequently N^2.

Now we can handle the general case. We will first check that $[N]$ is quasi-finite. Let $\overline{x}$ be a geometric point of S, we want to check that $[N]$ is non constant on $E_{\overline{x}}$ even when the characteristic of $\overline{x}$ divides N. We can choose $M \geqslant 2$ prime to the characteristic of $\overline{x}$. Then $[N]$ induces an automorphism of $\operatorname{Ker}[M]$ and we know that $\operatorname{Ker}[M]$ is non trivial since $[M]$ is étale of degree M^2. Consequently $[N]$ is a non constant map from $E_{\overline{x}}$ to $E_{\overline{x}}$, this scheme being irreducible of dimension 1, the map is finite flat. Consequently the endomorphism $[N]$ is a quasi-finite and proper map from E to E, hence a finite morphism. As E is a regular scheme, we can conclude that $[N]$ is a finite flat endomorphism of E

and since E is noetherian, locally free. By the previous computation we know that it has degree N^2. □

Corollary 5.21. *Let E/S be an elliptic curve. Let $N \in \mathbb{N}^*$. The group scheme $E[N]$ is finite locally free over S and it is étale if and only if $N \in \Gamma(S, \mathcal{O}_S)^\times$.*

5.6 Duals

An *isogeny* $f : E_1 \to E_2$ between S-elliptic curves is a finite locally free map such that $f(0) = 0$.

Let $f : E_1 \to E_2$ be an isogeny. For each S-scheme T, we have a commutative diagram

$$\begin{array}{ccc} E_1(T) & \longleftarrow & E_2(T) \\ \downarrow\wr & & \downarrow\wr \\ \mathrm{Pic}^0(E_{1,T}/T) & \xleftarrow[f_T^*]{} & \mathrm{Pic}^0(E_{2,T}/T) \end{array}$$

where f_T^* is the pullback along f_T. This pullback is naturally a group homomorphism and by functoriality we deduce that there exists an S-group schemes homomorphism $f^t : E_2 \to E_1$ inducing f_T^* on the T-points for all S-scheme T. This homomorphism is called the *dual map* of f.

Theorem 5.22. *Let $f : E_1 \to E_2$ be some isogeny of degree $N \geqslant 1$. Then f^t is an isogeny of degree N and $f^t \circ f = [N]$.*

Proof. We will first consider the case where $S = \operatorname{Spec} k$ with k some algebraic closed field. As f is flat, for all $P \in E(k)$, we have an isomorphism $f^*\mathcal{L}(P) \simeq \mathcal{L}(f^{-1}(P))$. Let switch to class groups. We have to prove the following relation in the class group of E :

$$[f^{-1}(f(P))] - [f^{-1}(0)] \sim N(P) - N(0).$$

We have an equality of finite subschemes $f^{-1}(f(P)) = P + f^{-1}(0)$. Moreover let $P_1, \dots P_r$ be the elements of the support of $f^{-1}(0)$. As f is finite locally free of degree N, we have $\deg[f^{-1}(0)] = N$ so that $[f^{-1}(0)] = \sum_i m_i(P_i)$ with $\sum_i m_i = N$. Then $[P + f^{-1}(0)] = \sum_i m_i(P + Q_i)$. Consequently we have

$$\begin{aligned} [f^{-1}(f(P))] - [f^{-1}(0)] &= \sum_i m_i(P + Q_i) - m_i(Q_) \\ &\sim \sum_i m_i(P) - m_i(0) = N(P) - N(0). \end{aligned}$$

The case of fields is proved. Before proving the general case, we need some intermediate results. □

I learned the following presentation of rigidity results in Brian Conrad's notes.

Lemma 5.23. *Let $p : X \to S$ and $q : Y \to S$ two S-schemes such that p is proper surjective of finite presentation with geometrically connected fibres. Assume that, for each geometrical point $\overline{s} \to S$, the application $f_{\overline{s}} : X_{\overline{s}} \to Y_{\overline{s}}$ is constant, then there exists a unique section $y \in Y(S)$ such that $f = y \circ p$.*

Proof. The map p is surjective and closed, hence it is a quotient map in the category of topological spaces. This implies that there exists a continuous map $y : S \to Y$ such that $f = y \circ p$. To upgrade y in a morphism of scheme, we need to define a morphism of sheaves $\mathcal{O}_Y \to y_*\mathcal{O}_S$. However we have a canonical isomorphism $\mathcal{O}_S \xrightarrow{\sim} p_*\mathcal{O}_X$ and a canonical isomorphism $y_*\mathcal{O}_S \xrightarrow{\sim} (y \circ p)_*\mathcal{O}_X = f_*\mathcal{O}_X$. It is natural to choose the composite $\mathcal{O}_Y \to f_*\mathcal{O}_X \xleftarrow{\sim} y_*\mathcal{O}_S$. We still have to check that this defines a map in the category of locally ringed spaces, more precisely that for each $y \in Y$, the induces map $\mathcal{O}_{Y,y} \to \mathcal{O}_{S,q(y)}$ is local. However choosing x in the fiber of p over $q(y)$, the composite

$$\mathcal{O}_{Y,y} \to \mathcal{O}_{S,q(y)} \to \mathcal{O}_{X,x}$$

which corresponds to f is local, this implies that the first map is local too. It is plain that, with these definitions, $f = y \circ p$. Unicity if left to the reader. □

Corollary 5.24. *Let $p : X \to S$ be some S-scheme proper and of finite presentation with geometrically connected fibres and let G be some S-group scheme. Let f and g two morphisms of S-schemes from X to G. Assume that, for all geometric point $\overline{s} \to S$, we have $f_{\overline{s}} = g_{\overline{s}}$ then there exists a section $y \in G(S)$ such that $g = (y \circ p)f$. Moreover, if there is some $x \in X(S)$ such that $f(x) = g(x)$, then $f = g$.*

End of the proof of Theorem 5.22. The two maps $[N]$ and $f^t \circ t$ coincides over each geometric point of S, consequently it follows from Corollary 5.24 that $[N] = f^t \circ f$. We have to check that f^t is flat. We know that $[N]$ is flat and f is flat and surjective (since it is on each fibre), consequently f is faithfully flat. This implies that f^t is flat and faithfully flat since it is surjective. Everything being of finite presentation, the map f^t is locally free, its degree can be deduced from the formula

$$\deg(f^t)\deg(f) = \deg(f^t \circ f) = \deg([N]) = N^2.$$

□

Theorem 5.25. *Let $f : E_1 \to E_2$ be some isogeny between S-elliptic curves. Then f is a morphism of S-group schemes.*

Proof. Let $N = \deg f$. It is sufficient to check that for P and Q in $E_2(S)$, then $f(P+Q) = f(P)+f(Q)$. We can fix $P \in E(S)$ and consider $g : E_1 \to E_2$ the morphism of S-schemes defined on points by $Q \mapsto g(Q) \coloneqq f(P+Q) - f(P) - f(Q)$. A direct computation, using the facts that f^t and $[N]$ are homomorphisms of S-group schemes shows that $f^t \circ g = 0$. Consequently the morphism g factors through the finite S-scheme $\operatorname{Ker} f^t$. A map of S-schemes from a proper S-scheme with geometrically connected fibres to an affine S-scheme is necessarily constant, hence $g = 0$. □

Unicity of the group law We will use the following rigidity result (cf. [KM85, Thm. 2.4.2]) :

Theorem 5.26. *Let S be a scheme and E_1 and E_2 two elliptic curves over S. Let f be a morphism of S-group schemes from E_1 to E_2. Then, Zariski locally on S, we have either $f = 0$ or f is finite locally free.*

Corollary 5.27. *Let $(E/S, 0)$ be an elliptic curve. There exists a unique structure of S-group scheme over E having 0 as neutral section.*

Proof. Let $m : E \times_S E \to E$ be the multiplication map of some S-group scheme structure on E having 0 for neutral section. Let $\mathcal{E}$ be the base change of E/S by $E \to S$, that is $\mathcal{E} = E \times_S E$. We define the endomorphism of E-scheme of $\mathcal{E}$ by $f(P, Q) = (P, m(P, Q) - P)$. This is clearly an automorphism of $\mathcal{E}/E$ sending 0 to 0 hence by Theorem 5.25 a morphism of E-group schemes. If $P \in E(S)$, we let f_P the automorphism of E induced by f along the base change $S \xrightarrow{P} E$. We conclude from Theorem 5.26 that the locus of $x \in E$ such that $f_x = \mathrm{Id}_E$ is open and closed. As $f_0 = \mathrm{Id}_E$ and that each connected component of E intersect the zero section, we conclude that $f = \mathrm{Id}_{\mathcal{E}}$ and consequently that $m(P, Q) = P + Q$ for all P, Q in $E(S)$. □

Remark 5.28. This result can also be deduced from Theorem 5.25.

Compatibility of duality and addition

Theorem 5.29. *Let E_1 and E_2 be two elliptic curves over S. Let f and g be two isogenies $E_1 \to E_2$. The $(f + g)^t = f^t + g^t$.*

Proof. It is enough to prove that, for $\mathcal{L}$ some invertible sheaf of degree 0 over E_2, then

$$(f + g)^* \mathcal{L} \simeq f^* \mathcal{L} \otimes g^* \mathcal{L}$$

in $\mathrm{Pic}(E_1/S)$. Viewing f and g as E_1-sections of the elliptic curve E_2, we are reduced to the case of some elliptic curve $f : E \to S$, P and Q two S-sections of E. It is therefore enough to prove that, for $\mathcal{L}$ an invertible sheaf of degree 0 over E, then

$$(P + Q)^* \mathcal{L} \otimes 0^* \mathcal{L} \simeq P^* \mathcal{L} \otimes Q^* \mathcal{L}.$$

The sheaf $\mathcal{L}$ is isomorphic to a sheaf of the form $\mathcal{L}(R) \otimes \mathcal{L}(0)^{-1} \otimes f^* \mathcal{L}_0$ for $\mathcal{L}_0$ some invertible sheaf over S. It is then a direct computation (see [KM85, Thm. 2.6.2]). □

Corollary 5.30. *We have $[N]^t = [N]$ for all $N \in \mathbb{Z}$.*

Proposition 5.31. *Let S be a scheme. Let $f : E_1 \to E_2$ and $g : E_1 \to E_3$ be two isogenies between elliptic curves over S. There exists an isogeny $h : E_2 \to E_3$ such that $g = h \circ f$ if and only if* $\mathrm{Ker}\, f \subset \mathrm{Ker}\, g$.

Proof. It is clear that the relation $g = h \circ f$ implies $\operatorname{Ker} f \subset \operatorname{Ker} g$. Conversely let us assume that $\operatorname{Ker} f \subset \operatorname{Ker} g$. We will consider in a first time the case where $E_2 = E_3$ and $f = [N]$ for some $N \geqslant 1$. Considering E_1-points, we have a commutative diagram

$$\begin{array}{ccc} E_1(E_1) & \xrightarrow{g_{E_1}} & E_2(E_1) \\ & {\scriptstyle N}\searrow \quad \nearrow{\scriptstyle \alpha} & \\ & E_2(E_1) & \end{array}$$

where g_{E_1} is a group homomorphism vanishing on the N-torsion, which implies the existence of a group homomorphism α such that $g_{E_1} = \alpha \circ N$. Let $h = \alpha(\mathrm{Id}_{E_1}) \in E_3(E_1)$. Then h is a morphism of S-schemes from E_1 to E_3. As $g_{E_1} = \alpha \circ N = N \circ \alpha = \underbrace{\alpha + \cdots + \alpha}_{N}$, we have

$$g = g_{E_1}(\mathrm{Id}_{E_1}) = \underbrace{h + \cdots + h}_{N} = [N] \circ h.$$

Then $h(0)$ is consequently an S-section of $\operatorname{Ker}[N]$. Replacing h by $h + h(0)$, we can assume that $h(0) = 0$. This implies that h is a group homomorphism and finally that

$$g = [N] \circ h = h \circ [N].$$

In the general case, the inclusion $\operatorname{Ker} f \subset \operatorname{Ker} g$ implies $\operatorname{Ker}(f \circ f^t) \subset \operatorname{Ker}(g \circ f^t)$. Since $f \circ f^t = [\deg f]$, the previous case shows the existence of h such that $g \circ f^t = h \circ f \circ f^t$. Now f^t being an isogeny is faithfully flat, hence an epimorphism in the category of schemes. This implies that $g = h \circ f$. □

Theorem 5.32. *Let S be a connected scheme and E an elliptic curve over S. Then the ring* $\operatorname{End} E$ *is a domain. Moreover if $f \in \operatorname{End} E$, there exists an integer* $\operatorname{Tr} f$ *such that $f + f^t = [\operatorname{Tr} f]$. In the domain* $\operatorname{End} E$*, the element f is annihilated by the polynomial $X^2 - (\operatorname{Tr} f)X + \deg f$ and we have the relation*

$$(\operatorname{Tr} f)^2 \leqslant 4 \deg f.$$

Proof. If f is a non zero element of $\operatorname{End} E$, the connectedness of S implies that f is an isogeny and consequently a surjective map. Consequently the composite of two non zero elements of $\operatorname{End} E$ is non zero. The relation

$$[\deg(f + \mathrm{Id}_E)] = (f + \mathrm{Id}_E) \circ (f^t + \mathrm{Id}_E) = [\deg f] + f + f^t + \mathrm{Id}_E$$

shows that we have to and can define

$$\operatorname{Tr} f \coloneqq \deg(f + \mathrm{Id}_E) - \deg f - 1.$$

Moreover if $(m, n) \in \mathbb{Z}^2$ such that $mf + n \neq 0$, then

$$0 \leqslant \deg(m + nf) = m^2 + mn \operatorname{Tr}(f) + n^2 \deg f.$$

This implies that for $\frac{m}{n} \in \mathbb{Q}$ such that $f + \frac{m}{n} \neq 0$, we have

$$\left(\frac{m}{n}\right)^2 + \frac{m}{n} \operatorname{Tr} f + \deg f \geqslant 0$$

which implies that the discriminant of this polynomial is non positive, that is

$$(\operatorname{Tr} f)^2 - 4 \deg f \leqslant 0.$$

The fact that f is annihilated by $X^2 - \operatorname{Tr}(f)X + \deg f$ is a direct computation. □

Corollary 5.33. *Let S be scheme and E some elliptic curve over S. Let f be some automorphism of E and let $N \geqslant 1$ be some integer such that $f|_{E[N]} = \mathrm{Id}_{E[N]}$. Then we have*

- *if $N \geqslant 3$, then $f = \mathrm{Id}_E$;*
- *if $N = 2$ and S is connected, then $f = \pm \mathrm{Id}_E$.*

Proof. We can assume that S is connected. As f is an automorphism, it has degree 1 so that $\operatorname{Tr} f \in \{0, \pm 1, \pm 2\}$. Moreover the inclusion $\operatorname{Ker}[N] \subset \operatorname{Ker}(f - \mathrm{Id}_E)$ implies the existence of some $g \in \operatorname{End} E$ such that

$$f = \mathrm{Id}_E + g \circ [N].$$

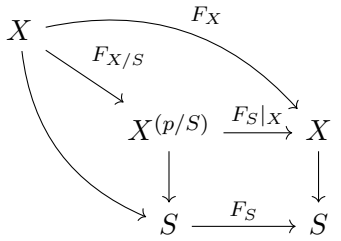
Taking trace and degree, we obtain the relations $\operatorname{Tr} f = 2 + N \operatorname{Tr} g$ and $1 = 1 + N \operatorname{Tr} g + N^2 \deg g$. These two relations and the inequality $N|\operatorname{Tr} g| \leqslant 4$ imply that $N^2 \deg g \leqslant 4$. Consequently if $N \geqslant 3$, we have $g = 0$ and $f = \mathrm{Id}_E$. Assume now that $N = 2$ and $f \neq \mathrm{Id}_E$. Then $g \neq 0$ and $\operatorname{Tr} g = -2$. We conclude that f is annihilated by the polynomial $(X + 1)^2$ and that $f = -\mathrm{Id}_E$. □

5.7 Frobenius morphism

Let p be a prime number and let X be a scheme of characteristic p. The *absolute Frobenius endomorphism* of X is the morphism of schemes F_X from X to X whose underlying continuous map is Id_X and acting on the structural sheaf by the ring endomorphism $x \mapsto x^p$. The formation of F_X is clearly functorial in X.

If X is an S-scheme with S of characteristic p, we define the S-scheme $X^{(p/S)}$ as the pullback of X along the absolute Frobenius endomorphism of S. The universal property of the fibre product of schemes implies that the absolute Frobenius F_X factors in $F_S|_X \circ F_{X/S}$ where $F_{X/S}$ is an S-morphism from X to $X^{(p/S)}$ which is called the *relative Frobenius homomorphism.* On a picture, we have the following commutative

diagram



Example 5.34. Let $S = \operatorname{Spec} k$ for some field k algebraically closed of characteristic 0 and let $X = \operatorname{Spec} k[x,y]/(y^2 - x^3 - ax - b)$. Then $X^{(p/S)} = \operatorname{Spec} k[x,y]/(y^2 - x^3 - a^p x - b)$ and the morphism $F_{X/S}$ acts on k points by the formula

$$\begin{array}{ccc} X(k) & \longrightarrow & X^{(p/S)}(k) \\ (x,y) & \longmapsto & (x^p, y^p). \end{array}$$

Of course if $F_S = \mathrm{Id}_S$ (as scheme morphisms), then $X^{(p/S)} = X$ and $F_{X/S} = F_X$.

In greater generality, if $q = p^f$ is some power of p, we define $F_X^q \coloneqq F_X^{\circ f}$ for X a scheme of characteristic p. We let $X^{(q/S)}$ be the pullback of some S-scheme X along F_S^q and F_X^q factors through $F_{X/S}^q$ from X to $X^{(q/S)}$.

Moreover if G is some S-scheme, then $F_{G/S}^q$ is a morphism of S-group schemes. In the particular case of an elliptic curve E/S, the morphism $F_{E/S}^q$ from E to $E^{(q/S)}$ is an isogeny of degree q which is never étale and annihilates the cotangent space $0^*\Omega^1_{E^{(q/S)}/S}$. The *Verschiebung* homomorphism is the dual isogeny $V_{E/S} \coloneqq F_{E/S}$ from $E^{(p/S)}$ to E. For q some power of p, we define $V_{E/S}^q \coloneqq (F_{E/S}^q)^t$. We have $V_{E/S}^q \circ F_{E/S}^q = [q]$ so that $V_{E/S}^q$ is an isogeny of degree q.

Theorem 5.35 (Hasse)**.** *Let q be some power of p and let $S = \operatorname{Spec} \mathbb{F}_q$. Let E be some elliptic curve over S, then we have*

$$|\operatorname{Card} E(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q}.$$

Proof. Let $\overline{\mathbb{F}_q}$ be an algebraic closure of $\mathbb{F}_q$. As $F_{E/S}^q$ acts trivially on the differential, the morphism $f \coloneqq \mathrm{Id}_E - F_E^q$ is étale. As a finite étale map, we have $\deg f = \operatorname{Card} \operatorname{Ker}(f|_{E(\overline{\mathbb{F}_q})})$. As F_E^q acts on $E(\overline{\mathbb{F}_q})$ as the q-Frobenius element of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, we conclude that

$$\operatorname{Card} E(\mathbb{F}_q) = \deg(\mathrm{Id}_E - F_E^q) = 1 + q - \operatorname{Tr}(F_E^q).$$

The inequality follows from

$$|\operatorname{Tr} F_E^q|^2 \leqslant 4 \deg F_E^q = 4q.$$

□

5.8 The Weil pairing

Let E/S be some elliptic curve and let $f : E_1 \to E_2$ be some isogeny. We will define a morphism of S-schemes

$$(-,-)_f : \operatorname{Ker} f \times_S \operatorname{Ker} f^t \to \mathbb{G}_{m,S}$$

such that, for all S-scheme T,

- the induced map on T-points is bilinear
$$\operatorname{Ker} f_T \times \operatorname{Ker} f_T^t \to \Gamma(T, \mathcal{O}_T)^\times;$$
- it is alternating :
$$\forall P \in \operatorname{Ker} f_T,\ \forall Q \in \operatorname{Ker} f_T^t, \quad (P,Q)_f (Q,P)_{f^t} = 1;$$
it is degenerate, it induces a isomorphism of S-group schemes
$$\operatorname{Ker} f \simeq \operatorname{Hom}_{S-\mathrm{gp}}(\operatorname{Ker} f^t, \mathbb{G}_{m,S});$$
- it is compatible to composition, that is, for another isogeny $g : E_2 \to E_3$, we have
$$\forall P \in \operatorname{Ker} f_T,\ \forall Q \in \ \operatorname{Ker}(f^t \circ g^t)_T, \quad (P,Q)_{g\circ f} = (P, g^t(Q))_f.$$

Moreover $(-,-)_f$ factors through $\mu_{N,S} \subset \mathbb{G}_{m,S}$ with $N = \deg f$.

The construction of the map is as followed on S-points. We use Abel isomorphism to identify $E_2(S)$ to $\operatorname{Pic}^0(E_2/S)$ and $\operatorname{Ker} f_S^t$ to the isomorphism classes of line bundles $\mathcal{L}$ on E_2 such that $f^*\mathcal{L} \simeq \mathcal{O}_{E_1}$. Note that the following diagram shows that each element in $\operatorname{Pic}^0(E_2/S)$ killed by f^* comes from a unique element of $\operatorname{Pic}^0(E_2)$ which is killed by f^*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Pic}(S) & \longrightarrow & \operatorname{Pic}^0(E_2) & \longrightarrow & \operatorname{Pic}^0(E_2/S) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle f^*} & & \\ 0 & \longrightarrow & \operatorname{Pic}(S) & \longrightarrow & \operatorname{Pic}^0(E_2) & \longrightarrow & \operatorname{Pic}^0(E_2/S) & \longrightarrow & 0. \end{array}$$

Then if $P \in \operatorname{Ker} f_S$ and $\mathcal{L} \in \operatorname{Ker} f^t$, we fix α an isomorphism between $f^*\mathcal{L} \simeq \mathcal{O}_{E_1}$. Then the sequence of isomorphisms

$$\mathcal{O}_{E_1} \xrightarrow[\alpha^{-1}]{\sim} f^*\mathcal{L} \xrightarrow[t_{-P}]{\sim}{}^* f^*\mathcal{L} \xrightarrow[t_{-P}^*\alpha]{\sim} \mathcal{O}_{E_1} \xrightarrow{\sim} \mathcal{O}_{E_1}$$

defines a global automorphism of $\mathcal{O}_{E_1}$. This automorphism is given by the multiplication by an element

$$(P,\mathcal{L})_f \in \Gamma(S, f_*\mathcal{O}_{E_1})^\times \simeq \Gamma(S, \mathcal{O}_S)^\times.$$

We refer to [Oda69, Thm. 1.1] for the checking of the predicted properties of the pairing. When $E_1 = E_2$ and $f = [N]$, we use the notation $e_N(P,Q)$ for $(P,Q)_{[N]}$. Moreover in this case the bilinearity proves that e_N factors through $\mu_{N,S}$ and we have, for f an endomorphism of E, for every S-scheme T and $(P,Q) \in E[N](T)$,

$$e_N(f(P),Q) = e_N(P, f^t(Q)), \qquad e_N(f(P), f(Q)) = e_N(P,Q)^{\deg f}.$$

5.9 The Tate module

The fundamental group Let S be a connected locally noetherian scheme. An *étale covering* of S is a finite étale scheme over S. Fix $\overline{s}$ a geometric point of S and let $F_{\overline{s}}$ be the covariant functor from the category of étale coverings of S to the category of finite sets sending X to $X_{\overline{s}} \coloneqq X \times_S \overline{s}$. It is proved in [SGA03, §V] that the automorphism group $\pi_1(S, \overline{s})$ of the functor $F_{\overline{s}}$ has a natural structure of profinite group so that $F_{\overline{s}}$ induces an equivalence of categories between the category of étale coverings of S and the category of finite sets endowed with a continuous action of $\pi_1(S, \overline{s})$. The profinite group $\pi_1(S, \overline{s})$ is called the *fundamental group* of the scheme S based at $\overline{s}$.

As a consequence, for two geometric points $\overline{s}$ and $\overline{s}'$, the groups $\pi_1(S, \overline{s})$ and $\pi_1(S, \overline{s}')$ are canonically isomorphic as are the functors $F \mapsto F_{\overline{s}}$ and $F \mapsto F_{\overline{s}'}$.

Example 5.36. Let $S = \operatorname{Spec} K$ for a field K and fix $\overline{s} = \operatorname{Spec} \overline{K}$ some algebraic closure of K. The finite étale coverings of K correspond to finite étale K-algebras and the functor $F_{\overline{s}}$ is the functor $\operatorname{Spec} A \mapsto \operatorname{Hom}_{K-\mathrm{alg}}(A, \overline{K})$. Then the fundamental group $\pi_1(S, \overline{s})$ is in this case the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K.

Let $f : S_1 \to S_2$ be a map of connected locally noetherian schemes and let $\overline{s}$ be some geometric point of S_1. The functor $F_{f \circ \overline{s}}$ is canonically isomorphic to $F_{\overline{s}} \circ f^*$. This implies that each automorphism of $F_{\overline{s}}$ induces an automorphism of $F_{f \circ \overline{s}}$ so that we obtain a group homomorphism

$$\pi_1(f) : \pi_1(S_1, \overline{s}) \to \pi_1(S_2, f \circ \overline{s}).$$

Example 5.37. Let S be a locally noetherian connected normal scheme and let $K \coloneqq k(S)$ be its fraction field. Let $\overline{K}$ be an algebraic closure of K giving rise to $\overline{s}$ a geometric point of S localised at $\operatorname{Spec} K$. Then the morphism

$$\mathrm{Gal}(\overline{K}/K) \to \pi_1(S, \overline{s})$$

is surjective and its kernel corresponds to the maximal Galois extension of K which is unramified at all codimension 1 points of S ([SGA03, Prop. V.8.2]).

Let S be locally noetherian scheme and let $\overline{s}$ be a geometric point of S. If G is a finite étale group scheme over S, then the fiber $G_{\overline{s}}$ is a finite group. Moreover the multiplication on G is a morphism of finite étale S-schemes $G \times_S G \to G$. It induces a morphism of groups $G_{\overline{s}} \times G_{\overline{s}} \to G_{\overline{s}}$ which commutes with the action of $\pi_1(S, \overline{s})$ (since $\pi_1(S, \overline{s})$ is the automorphism group of the *functor* $F \mapsto F_{\overline{s}}$). Conversely, it follows from the fact that $F \mapsto F_{\overline{s}}$ is an equivalence that the data of a finite group H with a continuous action of $\pi_1(S, \overline{s})$ (compatible with the group structure) comes from a unique, up to unique isomorphism, pair (G, i) where G is a finite étale group scheme G over S and i is a $\pi_1(S, \overline{s})$-equivariant group isomorphism $G_{\overline{s}} \simeq H$.

The Tate module of an elliptic curve Let S be locally noetherian connected scheme and let E/S be an elliptic curve. If $N \geqslant 1$ is some integer which is invertible on S, the S-group scheme $E[N]$ is finite étale over S and its geometric fibres are free $\mathbb{Z}/N\mathbb{Z}$-modules of rank 2. Consequently the datum of $E[N]$ is equivalent to the continuous linear action of $\pi_1(S, \overline{s})$ on $E[N](\overline{s}) \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

If ℓ is a prime number, invertible over S, the *Tate module* of E is the free $\mathbb{Z}_\ell$-module of rank 2 defined as

$$T_\ell E \coloneqq \varprojlim_n E[\ell^n](\overline{s})$$

where transition maps are $x \mapsto \ell x$. It is a finite free $\mathbb{Z}_\ell$-module with a continuous linear action of the profinite group $\pi_1(S, \overline{s})$. We also define its rational version $V_\ell E \coloneqq \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell E$ which is an ℓ-adic representation of dimension 2 of the profinite group $\pi_1(S, \overline{s})$.

Good reduction of elliptic curves Let K be a field, $v : K^\times \to \mathbb{Z}$ a discrete valuation on K and $\mathcal{O}_v$ its valuation ring. It follows from example 5.37 that the fundamental group of $\operatorname{Spec} \mathcal{O}_v$ is isomorphic to the quotient of the decomposition group of v by the inertial group at v. Let 's recall that this means the following : we fix some algebraic closure $\overline{K}$ of K and an extension $\overline{v}$ of v to $\overline{K}$ (which is not discrete anymore). Let k be the residue field of $\mathcal{O}_v$ and $\overline{k}$ the residue field of $\mathcal{O}_{\overline{v}}$. The *decomposition group* of $\overline{v}$ is the stabilizer $D_{\overline{v}}$ of $\overline{v}$ in $\operatorname{Gal}(\overline{K}/K)$ and the *inertia group* of $\overline{v}$ is the subgroup $I_{\overline{v}}$ of $D_{\overline{v}}$ acting trivially on $\overline{k}$. A representation of $\operatorname{Gal}(\overline{K}/K)$ is said to be *unramified at* v is the action of $I_{\overline{v}}$ is trivial for one, or equivalently any, extension $\overline{v}$ of v.

If E is an elliptic curve defined over K, we say that E has *good reduction* at v, if there exists an elliptic curve E_v over $\operatorname{Spec} \mathcal{O}_v$ and an isomorphism $E \simeq \operatorname{Spec} \mathcal{O}_v \times_{\operatorname{Spec} K} E_v$. As the ring $\mathcal{O}_v$ is normal, it follows from the description of its fundamental group that, for ℓ invertible on $\operatorname{Spec} \mathcal{O}_v$, the Galois representation over $V_\ell E$ is *unramified* at v.

Actually a reciprocal is true. The following result is called Néron-Ogg-Shavarevich criterion (see [ST68, Thm. 1]).

Theorem 5.38. *Let ℓ be a prime number which is invertible in k. Then an elliptic curve E over K has good reduction at v if and only if the action of* $\operatorname{Gal}(\overline{K}/K)$ *on $V_\ell E$ is unramified at v.*

In our situation it is known that we have a group isomorphism $D_{\overline{v}}/I_{\overline{v}} \simeq \operatorname{Gal}(\overline{k}/k)$. Moreover, if E has good reduction at v, the fibre of a E_v at $\operatorname{Spec} k$ is an elliptic curve over k denoted E_k. For ℓ invertible in k, we have a canonical isomorphism

$$T_\ell E \simeq T_\ell E_k$$

compatible with the homomorphism $D_{\overline{v}} \to \operatorname{Gal}(\overline{k}/k)$. Consequently the action of a decomposition group at v is completely determined by the *special fibre* E_k.

When k is a finite field, the group $\operatorname{Gal}(\overline{k}/k)$ is procyclic and topologically generated by a Frobenius automorphism.

Theorem 5.39. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Let* Frob_q *be the q-Frobenius automorphism of $\overline{\mathbb{F}_q}$ some algebraic closure of $\mathbb{F}_q$. Let ℓ be a prime number invertible in $\mathbb{F}_q$ and let ρ_ℓ group homomorphism* $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{GL}(V_\ell E)$*. Then the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_q)$ is*

$$X^2 - a_q X + q, \qquad a_q \coloneqq q + 1 - \mathrm{Card}\, E(\mathbb{F}_q).$$

It is very characteristic that this polynomial has integer coefficient and does not depend on the prime number ℓ. Moreover Hasse Theorem tells us that its roots in $\mathbb{C}$ are conjugate and have complex norm equal to $q^{\frac{1}{2}}$.

6 Models of modular curves

6.1 Moduli problems for elliptic curves

Let $[\mathcal{E}ll]$ be the contravariant functor from the category of schemes to the category of sets associating to a scheme S the set $[\mathcal{E}ll](S)$ of isomorphism classes of elliptic curves over S. A naive definition of the moduli space of elliptic curves would be the scheme representing the functor $[\mathcal{E}ll]$. Unfortunately this functor is not representable. Namely assume that we can represent it by some scheme X. This would mean the following : for each scheme S, there exists a functorial isomorphism

$$\mathrm{Hom}_{\mathrm{Sch}}(S, X) \simeq [\mathcal{E}ll](S).$$

In particular, if L/K is a field extension, the map $[\mathcal{E}ll](K) \to [\mathcal{E}ll](L)$ should be injective. This would imply that two elliptic curves defined over K which becomes isomorphic over L should be isomorphic. Here is however a counter example. Consider $K = \mathbb{Q}$ and $L = \overline{\mathbb{Q}}$ and, for $i \in \{1, 2\}$ let E_i be the elliptic curve defined by the Weierstrass equation

$$y^2 z = x^3 + (-1)^i z^3.$$

These two elliptic curves are isomorphic over $\overline{\mathbb{Q}}$, an isomorphism being

$$(x : y : z) \mapsto (-x : iy : z),$$

but they are not isomorphic over $\mathbb{Q}$. For example, we can check that $E_2[3](\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, generated by $(0, 1)$, but $E_1[3](\mathbb{Q}) = 0$ (check for example that $\mathrm{Card}\, E_1(\mathbb{F}_7) = 4$).

The non representability of this moduli problem is linked to the existence of non trivial isomorphisms of elliptic curves. A good approach to representability of moduli problems has to keep track of these automorphisms. There are several solutions to this problem. The first one is to add some "level structure" to elliptic curves so the objects we want to classify have no automorphisms. We can hope to be able to prove that the corresponding functor is representable. The other solution is to not add any structure

but to forget the idea to work with schemes and instead to work with a category of elliptic curves. The notion of "stack" achieves this task.

In this course, we will follow the classical textbook of Katz and Mazur ([KM85]) and adopt an intermediate position consisting to work with the stack of elliptic curves without telling it and use it to study moduli problems with level structure which may or may not be representable.

Let S be scheme. We define $\mathcal{E}ll_S$ as being the category whose objects are pairs (T, f) where T is an S-scheme and $f : E \to T$ is an elliptic curve over T. We will often use the notation $E_{/T}$ to denote such an object. A morphism from E_{1/T_1} to E_{2/T_2} in this category will be a cartesian diagram

$$\begin{array}{ccc} E_1 & \longrightarrow & E_2 \\ \downarrow & & \downarrow \\ T_1 & \longrightarrow & T_2 \end{array}$$

where the top horizontal arrow induces an isomorphism $E_1 \xrightarrow{\sim} E_2 \times_{T_2} T_1$ of elliptic curves over T_1.

A *moduli problem* is a contravariant functor $\mathcal{P}$ from the category $\mathcal{E}ll_S$ to the category of sets.

We will say that a moduli problem $\mathcal{P}$ is *relatively representable* if, for all $E_{/T}$ in $\mathcal{E}ll_S$, the presheaf on the category of T-schemes defined by $T' \mapsto \mathcal{P}(E_{T'/T'})$ is representable by a scheme $\mathcal{P}_{E_{/T}}$.

Let P be a property of morphism of schemes which is stable under base change. We will say that a relatively representable moduli problem $\mathcal{P}$ has property P if, for all $E_{/T}$, the map $\mathcal{P}_{E_{/T}} \to T$ has property P.

We say that a moduli problem is *representable* if the functor $\mathcal{P}$ is representable by some object $\mathbf{E}_{/\mathcal{M}(\mathcal{P})}$ in the category $\mathcal{E}ll_S$. If $\mathcal{P}$ is representable, the S-scheme $\mathcal{M}(\mathcal{P})$ represents the presheaf

$$\begin{array}{ccc} \mathrm{Sch}_S^{\mathrm{op}} & \to & \mathrm{Sets} \\ T & \mapsto & \{(E_{/T}, a) \mid a \in \mathcal{P}(E_{/T})\}_{/\simeq}. \end{array}$$

Examples of moduli problems Let S be a scheme and let $N \in \mathbb{N}^*$ be invertible over S. Let $E_{/S}$ be an elliptic curve. A *full level N structure* over S is an isomorphism of locally finite group schemes

$$(\mathbb{Z}/N\mathbb{Z})_S^2 \simeq E[N].$$

We denote by $[\Gamma(N)](E_{/S})$ be the set of all full level N structures over E. We obtain a presheaf $E_{/T} \mapsto [\Gamma(N)](E_{/T})$ over $\mathcal{E}ll_S$. This is our first example of moduli problem.

We can define some other moduli problems $[\Gamma_1(N)]$ and $[\Gamma_0(N)]$ over $\mathcal{E}ll_S$. We define $[\Gamma_1(N)](E_{/S})$ as the set of all monomorphisms of finite étale group schemes $(\mathbb{Z}/N\mathbb{Z})_S \hookrightarrow$

$E[N]$ and $[\Gamma_0(N)](E_{/S})$ as the set of all closed subgroup schemes $H \subset E[N]$ such that for all geometric point $\overline{s} \to S$, the fiber $H_{\overline{s}}$ is cyclic of order N. It is plain that $[\Gamma_1(N)]$ and $[\Gamma_0(N)]$ are examples of moduli problems. Note that we can identify $[\Gamma_1(N)](E_{/S})$ with the set of all sections of $E[N]$ which are of order N at each geometric point.

Proposition 6.1. *If N is invertible over S, the three moduli problems $[\Gamma(N)]$, $[\Gamma_1(N)]$ and $[\Gamma_0(N)]$ are relatively representable and finite étale.*

Proof. We will begin by the proof that $[\Gamma(N)]$ is relatively representable. It is sufficient to prove that it is representable in the case where S is a connected scheme. In this case, the data of a morphism from the constant group $(\mathbb{Z}/N)^2_S$ to $E[N]$ is equivalent to the data of group homomorphism

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](S).$$

Such a group homomorphism is determined by the two sections corresponding to the images of elements of a basis of $(\mathbb{Z}/N\mathbb{Z})^2$, let say $\alpha(1,0)$ and $\alpha(0,1)$. Consequently the functor $[\Gamma(N)]$ is a subfunctor of the functor $E[N] \times_S E[N]$. Recall that the Weil pairing e_n induces a perfect pairing

$$E[N](S) \times E[N](S) \to \mu_N(S).$$

so that two elements u and v of $E[N](S)$ generates the groupe $E[N](S)$ if and only if $e_N(u,v)$ is a primitive root of unity, that is an element of order N in $\mu_N(S)$. Let $\mu_N^\times \subset \mu_N$ be the subfunctor of μ_N consisting of primitive roots of unity. It is represented by a closed subcheme of μ_N. Namely μ_N is represented by the scheme $\operatorname{Spec} \mathcal{O}_S[X]/(X^N - 1)$ and $\mu_N^\times$ by the scheme $\operatorname{Spec} \mathcal{O}_S[X]/(\Phi_N(X))$ where $\Phi_N(X)$ is the N-th cyclotomic polynomial. We conclude that the set $[\Gamma(N)](E_{/S})$ is the set of sections of the closed subscheme of $E[N] \times_S E[N]$ defined as the inverse image of $\mu_N^\times$ under $e_N : E[N] \times_S E[N] \to \mu_N$. This proves that $[\Gamma(N)]$ is relatively representable and that

$$[\Gamma(N)]_{E_{/S}} \simeq (E[N] \times_S E[N]) \times_{\mu_N} \mu_N^\times.$$

As $[\Gamma(N)]_{E_{/S}}$ is a closed subscheme of the finite étale S-scheme $E[N] \times_S E[N]$, it is finite over S. As the map $\mu_N \to S$ is étale, it follows from Proposition 4.10 that the map e_N is étale and, by base change, that $[\Gamma(N)]_{E_{/S}} \to \mu_N^\times$ is étale. As $\mu_N^\times \to S$ is étale too, so is $[\Gamma(N)]_{E_{/S}} \to S$. The two other cases are similar. □

Rigid moduli problems Let $\mathcal{P}$ be a moduli problem on the category $\mathcal{E}ll_S$, we say that $\mathcal{P}$ is *rigid* if for $E_{/T}$ an object of $\mathcal{E}ll_S$ and $\alpha \in \mathcal{P}(E_{/T})$ and φ an automorphism of $E_{/T}$, if $\varphi^*(\alpha) = \alpha$, then $\varphi = \mathrm{Id}$.

If $\mathcal{P}$ is a representable moduli problem, then it is rigid. Namely assume that $\mathcal{P}$ is representable by $\mathbf{E}_{/\mathcal{M}}$ and let φ be an automorphism of some elliptic curve fixing some $\alpha \in \mathcal{P}(E_{/T})$. Then the pair $(E_{/T}, \alpha)$ corresponds to some unique morphism f :

$E_{/T} \to \mathbf{E}_{/\mathcal{M}}$. However by definition $f \circ \varphi$ gives rise to the same element $\alpha \in \mathcal{P}(E_{/T})$. Consequently $f \circ \varphi = f$. However, f being a base change morphism, we have $\varphi = \mathrm{Id}_E$.

Consequently the existence of the automorphism $[-1]$ shows that the functors $[\Gamma_0(N)]$, or $[\Gamma(N)]$ for $N \leqslant 2$ cannot be representable. In a positive direction, we will prove a bit later :

Theorem 6.2. *Let S be a scheme and let $\mathcal{P}$ be a relatively representable affine and rigid moduli problem. Then $\mathcal{P}$ is representable.*

6.2 Examples of representable moduli problems

Proposition 6.3. *Let S be a scheme over $\operatorname{Spec}\mathbb{Z}[\frac{1}{2}]$. Let $(E/S, 0)$ be some elliptic curve and $P \in E[4](S)$ a section of order 4 over each connected component of S. Then there exists a unique $d \in \Gamma(S, \mathcal{O}_S)^\times$ and a unique isomorphism of elliptic curves*

$$f : (E/S, 0) \xrightarrow{\sim} E_d \coloneqq \left(\operatorname{Proj}_S \mathcal{O}_S[x, y, z]/(dy^2z - x^3 - (d-2)x^2z - xz^2), (0:1:0)\right)$$

such that $d(d-4) \in \Gamma(S, \mathcal{O}_S)^\times$ and $f(P) = (1:1:1)$ and $f([2](P)) = (0:0:1)$.

Proof. The unicity of f is a consequence of the rigidity of the moduli problem $[\Gamma_1(4)]$. The unicity of d comes from the fact that an isomorphism of elliptic curves between E_d and $E_{d'}$ is necessarily of the form $(x : y : z) \mapsto (ax + bz : cy : z)$. However if such an isomorphism fixes $(1:1:1)$ and $(0:0:1)$ we have $a = c = 1$ and $b = 0$, so that $d = d'$.

Having unicity we can just prove existence of d and f locally on S, everything can then be glued. Consequently we can assume that $S = \operatorname{Spec} A$ and E is given by some Weierstrass equation of parameter $(a_1, a_2, a_3, a_4, a_6)$. As $2 \in A^\times$, we can make a change of variable so that $a_1 = a_3 = 0$ and we can ask that $[2](P) = (0:0:1)$ so that $a_6 = 0$. Let $P = (x_P : y_P : 1)$. As $E[4]$ is finite étale over S, the section P is of order 4 at each geometric point of S, so that $(x_P, y_P) \in (\Gamma(S, \mathcal{O}_S)^\times)^2$. This implies that we can rescale the variables x and y so that $x_P = y_P = 1$. Then E has a Weierstrass equation of the form

$$dy^2z = x^3 + a_2x^2z + a_4xz^2$$

with $d \in \Gamma(S, \mathcal{O}_S)^\times$. As P has order 4, the invertible sheaf $\mathcal{M} \coloneqq \mathcal{L}(3(0) - 2(P) - ([2]P))$ is isomorphic to the pullback of an invertible sheaf on S. We are free to shrink S and to assume that $\mathcal{M}$ is trivial. We conclude that $p_*\mathcal{M}$ (where $p : E \to S$) is free of rank 1. From compatibility with base change, it is isomorphic to $p_*\mathcal{L}(3(0) - (P) - ([2]P))$ and to a direct factor $p_*\mathcal{L}(3(0))$. We can conclude that $y - x$ is a generator of its global sections. This implies the equality

$$x^3 + a_2x^2 + a_4x - dx^2 = x(x-1)^2$$

giving $a_4 = 1$ and $a_2 - d = -2$. The condition $d(d-4) \in \Gamma(S, \mathcal{O}_S)^\times$ is then the precise condition to obtain a smooth curve over S. □

Corollary 6.4. *The moduli problem* $[\Gamma_1(4)]$ *over* $\mathcal{E}ll_{\mathbb{Z}[\frac{1}{2}]}$ *is representable by the pair* $(\mathbf{E}, P)$ *where* $\mathbf{E}$ *is the elliptic curve defined by*

$$dy^2z = x^3 + (d-2)x^2 + x$$

over the scheme $\mathcal{M}(\Gamma_1(4)) = \operatorname{Spec}\mathbb{Z}\left[\frac{1}{2}, d, (d(d-4))^{-1}\right]$ *and* $P \in \mathbf{E}[4](\mathcal{M}(\Gamma_1(4)))$ *is the section of homogeneous coordinates* $(1:1:1)$.

Corollary 6.5. *The functor* $[\Gamma(4)]$ *over* $\mathcal{E}ll_{\mathbb{Z}[\frac{1}{2}]}$ *is representable.*

Proof. Let $(\mathbf{E}/\mathcal{M}(\Gamma_1(4)), P)$ be the elliptic curve with point of order 4 representing $[\Gamma_1(4)]$. Let's consider the morphism of $\mathcal{M}(\Gamma_1(4))$ schemes

$$e_4(P, -) : \mathbf{E}[4] \to \mu_{4,\mathcal{M}(\Gamma_1(4))}$$

and let $\mathcal{M}(\Gamma(4))$ be the inverse image of $\mu_4^\times$ the closed subschemes of primitive roots of unity. Let $\mathbf{E}'$ be the inverse image of $\mathbf{E}$ on $\mathcal{M}(\Gamma(4))$ and P_1 the pullback of P as a section of $\mathbf{E}'[4]$. We define $P_2 \in \mathbf{E}'[4](\mathcal{M}(\Gamma_1(4))$ coming from the tautological section $\mathcal{M}(\Gamma(4)) \to \mathbf{E}[4]$. The pair (P_1, P_2) is a $\Gamma(4)$-structure on $\mathbf{E}'$ and the triple $(\mathbf{E}', P_1, P_2)$ obviously represents the functor $[\Gamma(4)]$. □

Let E/S be some elliptic curve. A full level 3 structure over E is an isomorphism of group schemes between the constant groupe scheme $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})_S$ and $E[3](S)$. Such an isomorphism is characterized by a group homomorphism

$$\alpha : (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \to E(S)$$

or equivalently by two section $P_1 = \alpha(1, 0)$ and $P_2 = \alpha(0, 1)$.

Proposition 6.6. *Let* S *be a scheme over* $\operatorname{Spec}\mathbb{Z}\left[\frac{1}{3}\right]$. *Let* E/S *be some elliptic curve over* S. *Let* (P_1, P_1) *be some full level* 3 *structure over* E. *Then there exists unique section* $B, C \in \Gamma(S, \mathcal{O}_S)^\times$ *such that* $B^3 = (B+C)^3$ *and a unique isomorphism of elliptic curves from* E *to*

$$\operatorname{Proj}_S \mathcal{O}_S[x, y, z]/(y^2z + a_1xyz + a_3yz^2 - x^3)$$

with $a_1 = 3C - 1$ *and* $a_3 = -3C^2 - 3BC - B$ *sending* P_1 *onto* $(0:0:1)$ *and* P_2 *onto* $(C : B + C : 1)$. *Moreover we have* $Ca_3(a_1^2 - 27a_3^2) \in \Gamma(S, \mathcal{O}_S)^\times$.

Proof. The unicity is analogous to the case of Proposition 6.3. We have essentially to prove the existence and we can work locally on S and assume that $S = \operatorname{Spec} A$ and E is given by an equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6.$$

Up to a change a variable, we can assume that $P_1 = (0 : y_{P_1} : 1)$. Moreover, P_1 being a section of order 3, we can assume, up to shrinking S, that $\mathcal{L}(3(0) - 3(P_1))$ is trivial and that there exists unique a and b in A such that $y + ax + b \in \Gamma(S, p_*\mathcal{L}(3(0) - 3(P_1))$. Replacing y by $y + ax + b$ we obtain a new equation which is of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3.$$

Moreover there exists a' and b' such that $y + a'x + b'$ generates $\Gamma(S, p_*\mathcal{L}(3(0) - 3(P_2))$. As (P_1, P_2) is a full level 3 structure, we have $P_2 \neq \pm P_1$ after evaluation at each geometric point of S, consequently a direct computation over an algebraically closed field of characteristic different from 3 shows that $a' \in \Gamma(S, \mathcal{O}_S)^\times$. We can then make a change of variable so that E has an equation of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 \tag{6}$$

with $P_1 = (0, 0)$ and $y - x - B \in \Gamma(S, p_*\mathcal{L}(3(0) - 3(P_2))$ so that $P_2 = (C, B + C)$ for some $C \in \Gamma(S, \mathcal{O}_S)^\times$ (to see that C is invertible, check it at each geometric point). Then, replacing y by $x + B$ in (6), we have

$$x^3 - (x + B)^2 - a_1(x + B)x - a_3(x + B) = (x - C)^3$$

which gives

$$\begin{cases} 3C & = 1 + a_1 \\ -3C^2 & = 2B + a_1B + a_3 \\ C^3 & = B^2 + a_3B \end{cases} \Rightarrow \begin{cases} a_1 & = 3C - 1 \\ a_3 & = -3C^2 - 3BC - B \\ B^3 & = (B + C)^3 \end{cases}.$$

Finally a direct computation shows that the equation (6) defines a smooth curve over S if and only if $a_3(a_1^2 - 27a_3^3) \in \Gamma(S, \mathcal{O}_S)^\times$. □

Corollary 6.7. *The moduli problem* $[\Gamma(3)]$ *is representable over* $\mathcal{E}ll_{\mathbb{Z}[\frac{1}{3}]}$ *by the triple* $(\mathbf{E}, P_1, P_2)$ *where* $\mathbf{E}$ *is the elliptic curve of equation*

$$y^2z + a_1xyz + a_3yz^2 = x^3$$

over $\mathcal{M}(\Gamma(3)) \coloneqq \operatorname{Spec} \mathbb{Z}\left[\frac{1}{3}, B, C, (Ca_3(a_1^2 - 27a_3^2))^{-1}\right]/(B^3 - (B + C)^3)$ *and* $P_1 = (0 : 0 : 1)$, $P_2 = (C : B + C : 1)$.

6.3 Quotients by a finite group

A reference for the results recalled in this section is [SGA03, exp V, §1,2].

Let X be a scheme and let G be a finite group acting on S. A morphism of scheme $p : X \to Y$ is a *quotient* of X by G if it has the following properties

- for all $g \in G$, $p \circ g = p$;

- the map p is a quotient in the category of topological spaces ;
- the map $\mathcal{O}_Y \to p_*\mathcal{O}_X$ induces an isomorphism of sheaves $\mathcal{O}_Y \xrightarrow{\sim} p_*\mathcal{O}_X^G$.

If $p : X \to Y$ is a quotient, then the scheme Y represents the functor $\mathrm{Hom}(X, -)^G$, the map p is consequently unique up to unique isomorphism and is called the quotient of X by G and we write $Y = G\backslash X$.

If $X = \mathrm{Spec}\, A$ is affine, let $B = A^G$. Then the map of schemes $\mathrm{Spec}\, A \to \mathrm{Spec}\, B$ is a quotient. Moreover if C is a flat B-algebra, then $C \xrightarrow{\sim} (A \otimes_B C)^G$ so that the formation of quotient commutes to flat base change.

Proposition 6.8. *Let X be a scheme and G a finite group acting on X. Then the quotient of X by G exists if and only if every orbit of G is contained in an open affine subset of X.*

Proof. See [SGA03, Prop. V.1.8]. □

Concerning the finitness properties of the quotient we have ([SGA03, Cor. V.1.5]) :

Proposition 6.9. *Let Z be a scheme and let X be some Z-scheme and G a finite group acting on X by automorphism of Z-schemes and let $X \to Y$ be a quotient. If X is of finite type over Z, then X is finite over Y. Morever if Z is locally noetherian, then Y is of finite type over Z.*

Decomposition and inertia groups Let X be a scheme and let G be a group acting on X. If $x \in X$, the *decomposition subgroup* at x is the stabilizer $G_d(x)$ of x. The *inertia subgroup* at x is the kernel of $G_d(x) \to \mathrm{Aut}(k(x))$.

Proposition 6.10. *Let X be a scheme and G be a finite group acting on X. Assume that the quotient $Y \coloneqq G\backslash X$ exists. If $G_i(x) = \{e\}$, then the quotient map p is étale at x. Conversely if moreover X is connected and G acts faithfully on X, then p étale at x implies $G_i(x) = \{e\}$.*

Proof. See [SGA03, Prop. 2.2 & Cor. 2.4]. □

Étale G-torsors Let $X \to Y$ be morphisme and scheme. Let G be a finite group acting on X via automorphisms over Y. We say that the action of G on X is locally trivial if, locally for the Zariski topology on Y, X is isomorphic to the product $G \times Y$ with action of G given by $g \cdot (h, y) = (gh, y)$. When Y is a quotient of X by G, it is very unlikely that X is locally trivial over Y. However if we replace the Zariski topology by the étale topology, it can often be the case. We won't define here formally the étale topology which is not a usual topology but a Grothendieck topology. Instead we will use the notion of étale G-torsor as defined below.

Proposition 6.11. *Let Y be a locally noetherian scheme, X a scheme over Y and G a finite group acting on X by Y-automorphisms. The following assertions are equivalent*

(i) the scheme X is finite over Y, the quotient of X by G exists and is isomorphic to Y and all inertia groups of G are trivial ;

(ii) there exists a surjective finite étale map $Y_1 \to Y$ such that, if $X_1 \coloneqq X \times_Y Y_1$, there exists a G-equivariant isomorphism of Y_1-schemes between X_1 and $G \times Y_1$.

Proof. See [SGA03, Prop. 2.6]. □

If X satisfies the equivalent properties of Proposition 6.11, we say that X is an *étale G-torsor* over Y.

Descent for étale G-torsors Let $X \to Y$ be a quotient map for a finite group G. If Z is an "object" over Y, ie a sheaf or a scheme, we can pull back Z to X to obtain an object over X endowed with an action of G. The problem of "descend" is to give some explicit criterion characterizing the G-equivariant objects over X obtained by this process. We will focus on the case where $X \to Y$ is an étale G-torsor.

Let G be some finite group and let $S' \to S$ be some étale G-torsor. If X' is some S'-scheme, a *descent data* over X' relative to S' is an action of G on X' such that the structure map $X' \to S'$ is G-equivariant. If moreover $\mathcal{F}'$ is a coherent sheaf over X', a descent data over the pair $(X', \mathcal{F}')$ is a descent data on X' and, for each $g \in G$ an isomorphism $\theta_g : g^*\mathcal{F}' \xrightarrow{\sim} \mathcal{F}'$ such that $\theta_{gh} = \theta_h \circ h^*\theta_g$.

If X is an S-scheme, then the pullback $X' = X \times_S S'$ has a natural descent data. An element $g \in G$ acts on X' by $\mathrm{Id}_X \times g$. Let $\mathcal{F}$ be a coherent sheaf X. Let $\mathcal{F}'$ be the pullback of $\mathcal{F}$ on X'. Then $\mathcal{F}'$ has a natural descent data given by

$$\theta_g \otimes \mathrm{Id}_{\mathcal{F}} : g^*\mathcal{F}' \simeq \mathcal{O}_{S'} \otimes_{\mathcal{O}_S} \mathcal{F} \xrightarrow{\sim} \mathcal{O}_{S'} \otimes_{\mathcal{O}_S} \mathcal{F}.$$

Theorem 6.12. *Let $S' \to S$ be an étale G-torsor.*

(i) The functor $X \mapsto X'$ from the category of affine schemes over S to the category of affine schemes with descent data over S' is an equivalence of categories.

(ii) The functor $(X, \mathcal{L}) \mapsto (X', \mathcal{L}')$ from the category of pairs $(X, \mathcal{F})$ where X is a projective S-scheme and $\mathcal{L}$ a relatively ample invertible sheaf over X to the category of similar pairs with descent data over S' is an equivalence of categories.

Proof. This can be proved directly or as a consequence of a more general result for maps $S' \to S$ which are faithfully flat and quasicompact ([SGA03, Thm. VIII.2.1] and [SGA03, Prop. VIII.7.8]). □

Example 6.13. If E' is some elliptic curve over S' with a descent data *compatible with the structure of elliptic curve*, then E' descends to an elliptic curve over S. Namely we can apply Theorem 6.12 with the relatively ample invertible sheaf $\mathcal{L}(0)$.

6.4 Proof of the representability theorem 6.2

In this section, we prove Theorem 6.2.

Let $\mathcal{P}$ be some moduli problem over $\mathcal{E}ll_S$. We say that a finite group G acts on $\mathcal{P}$ if for each object $E_{/T}$ in $\mathcal{E}ll_S$, there is an action of G on the set $\mathcal{P}(\mathcal{E}ll_{/T})$ and if the transition maps $\mathcal{P}(E_{/T}) \to \mathcal{P}(E'_{/T'})$ are G-equivariant.

Lemma 6.14. *Let S be a locally noetherian scheme. Let $\mathcal{P}$ be some moduli problem over $\mathcal{E}ll_S$ which is affine and rigid. Let G be a finite group and let $\mathcal{Q}$ be an other moduli problem over $\mathcal{E}ll_S$ such that*

- *the functor $\mathcal{Q}$ is representable by an elliptic curve $\mathbf{E}(\mathcal{Q})_{/\mathcal{M}(\mathcal{Q})}$ over an affine S-scheme $\mathcal{M}(\mathcal{Q})$;*
- *the group G acts on $\mathcal{Q}$ and tor each $E_{/T}$ in $\mathcal{E}ll_S$, the T-scheme $\mathcal{Q}_{E_{/T}}$ representing the $\mathcal{Q}$-structures on $E_{/T}$ is an étale G-torsor over T.*

Then the functor $\mathcal{P}$ is representable.

Proof. The functor $\mathcal{P}$ is relatively representable and the functor $\mathcal{Q}$ is representable. This implies that the functor $\mathcal{P} \times \mathcal{Q}$ is representable. Namely it is easy to check that it is representable by the base change $\widetilde{\mathbf{E}}$ of $\mathbf{E}(\mathcal{Q})_{/\mathcal{M}(\mathcal{Q})}$ to $\mathcal{M}(\mathcal{P},\mathcal{Q}) \coloneqq \mathcal{P}_{\mathbf{E}(\mathcal{Q})/\mathcal{M}(\mathcal{Q})}$. The group G acts on $\mathcal{Q}$, consequently it acts on $\mathcal{M}(\mathcal{Q})$, $\mathbf{E}(\mathcal{Q})$, $\mathcal{M}(\mathcal{P},\mathcal{Q})\ldots$ The inertia groups of G acting on $\mathcal{M}(\mathcal{P},\mathcal{Q})$ are trivial. Namely it is sufficient to check that G acts freely on the functor of points of $\mathcal{M}(\mathcal{P},\mathcal{Q})$. Let $\operatorname{Spec} A$ be an affine S-scheme. Then

$$\mathcal{M}(\mathcal{P},\mathcal{Q})(A) \simeq \{(E_{/\operatorname{Spec} A}, \alpha, \beta) \mid (\alpha,\beta) \in \mathcal{P}(E_{/\operatorname{Spec} A}) \times \mathcal{Q}(E_{/\operatorname{Spec} A})\}/\simeq .$$

Let $g \in G$. If $g(E_{/\operatorname{Spec} A}, \alpha, \beta) \simeq (E_{/\operatorname{Spec} A}, \alpha, \beta)$, there exists an automorphism φ of E such that $\varphi^*(\alpha) = \alpha$ and $\varphi^*(\beta) = g\beta$. As $\mathcal{P}$ is rigid, we have $\varphi = \mathrm{Id}_E$ so that $g\beta = \beta$. However, $\mathcal{Q}_{E_{/\operatorname{Spec} A}} \to \operatorname{Spec} A$ is a G-torsor and $\mathcal{Q}(E_{/\operatorname{Spec} A})$ coincides with the set of sections of this map. Therefore if $g\beta = \beta$ we have $g = e_G$. This proves that the action of G is faithful on the functor $\mathcal{P} \times \mathcal{Q}$.

The moduli problem $\mathcal{P}$ being relatively representable and affine, the scheme $\mathcal{M}(\mathcal{P},\mathcal{Q})$ is affine over $\mathcal{M}(\mathcal{Q})$ and $\mathcal{M}(\mathcal{Q})$ is affine. This implies that $\mathcal{M}(\mathcal{P},\mathcal{Q})$ is affine over S. Hence the quotient $G\backslash\mathcal{M}(\mathcal{P},\mathcal{Q})$ exists and it follows from Proposition 6.11 that the map $\mathcal{M}(\mathcal{P},\mathcal{Q}) \to G\backslash\mathcal{M}(\mathcal{P},\mathcal{Q})$ is an étale G-torsor. We now define

$$\mathcal{M}(\mathcal{P}) \coloneqq G\backslash\mathcal{M}(\mathcal{P},\mathcal{Q}).$$

As G acts on $\widetilde{\mathbf{E}}$, there is a descent data on $\widetilde{\mathbf{E}}$ and it follows from example 6.13 that this elliptic curves descends along $\mathcal{M}(\mathcal{P},\mathcal{Q}) \to G\backslash\mathcal{M}(\mathcal{P},\mathcal{Q})$. Let $\mathbf{E}$ be the elliptic curve over $\mathcal{M}(\mathcal{P})$ obtained by this descent process.

Let $\widetilde{\alpha_{\text{univ}}} \in \mathcal{P}(\widetilde{\mathbf{E}})$ be the universal $\mathcal{P}$-structure over $\widetilde{\mathbf{E}}$, ie the first component of the element $(\widetilde{\alpha_{\text{univ}}}, \widetilde{\beta_{\text{univ}}})$ corresponding to the identity map of $\widetilde{\mathbf{E}}$. We want to prove that it is the image of a unique element $\alpha_{\text{univ}} \in \mathcal{P}(\mathbf{E}_{/\mathcal{M}(\mathcal{P})})$ by $\mathcal{P}(\mathbf{E}_{/\mathcal{M}(\mathcal{P})}) \to \mathcal{P}(\widetilde{\mathbf{E}}_{/\mathcal{M}(\mathcal{P},\mathcal{Q})})$. This will follow from the fact that the map

$$\mathcal{P}(\mathbf{E}_{/\mathcal{M}(\mathcal{P})}) \to \mathcal{P}(\widetilde{\mathbf{E}}_{/\mathcal{M}(\mathcal{P},\mathcal{Q})})$$

is injective with image the subset of the fixed points of G. Consider the map $\mathcal{Q}_{\mathbf{E}_{/\mathcal{M}(\mathcal{P})}} \to \mathcal{M}(\mathcal{P})$. The base change of $\mathbf{E}$ to $\mathcal{Q}_{\mathbf{E}_{/\mathcal{M}(\mathcal{P})}}$ admits a canonical $\mathcal{Q}$-structure corresponding to a map

$$\mathcal{Q}_{\mathbf{E}_{/\mathcal{M}(\mathcal{P})}} \to \mathcal{M}(\mathcal{P},\mathcal{Q})$$

so that we have a G-equivariant commutative diagram

$$\begin{array}{ccc} \mathcal{Q}_{\mathbf{E}_{/\mathcal{M}(\mathcal{P})}} & \longrightarrow & \mathcal{M}(\mathcal{P},\mathcal{Q}) \\ & \searrow \quad \swarrow & \\ & \mathcal{M}(\mathcal{P}) & \end{array} .$$

However both vertical maps are étale G-torsors. This implies that the horizontal map is an isomorphism (it is finite étale of degree 1). Consequently, as a G-set, $\mathcal{P}(\widetilde{\mathbf{E}}_{/\mathcal{M}(\mathcal{P},\mathcal{Q})})$ is isomorphic to

$$\mathcal{P}(\mathbf{E}_{/\mathcal{Q}_{\mathbf{E}_{/\mathcal{M}(\mathcal{P})}}}) \simeq \mathcal{P}(\mathbf{E}_{/\mathcal{M}(\mathcal{P})}) \times \mathcal{Q}(\mathbf{E}_{/\mathcal{M}(\mathcal{P})}).$$

This proves our assertion.

The functor $\mathcal{P}$ being relatively representable and affine, the elements $\mathcal{P}(E_{/T})$ are in bijection with the section of the affine scheme $\pi : \mathcal{P}_{E_{/T}} \to T$ consequently $\mathcal{P}(E_{/T})$ corresponds to the global section of the quasicoherent sheaf $\pi_*\mathcal{O}_{\mathcal{P}_{E_{/T}}}$. The element $\widetilde{\alpha_{\text{univ}}}$ corresponds to a G-invariant section of the quasicoherent sheaf $f^*\pi_*\mathcal{O}_{\mathcal{P}_{\mathbf{E}_{/\mathcal{M}(\mathcal{P})}}}$ over $\mathcal{M}(\mathcal{P},\mathcal{Q})$ consequently it descends uniquely to $\mathcal{M}(\mathcal{P})$.

Now we have to check that the $\mathbf{E}_{/\mathcal{M}(\mathcal{P})}$ represents $\mathcal{P}$ with universal class α_{univ} ie that for all $\alpha \in \mathcal{P}(E_{/T})$, there is a unique morphism of S-schemes $T \to \mathcal{M}(\mathcal{P})$ such that E is isomorphic to the pullback of $\mathbf{E}$ and such that α_{univ} is sent on α.

Let $(E_{/T}, \alpha)$ with $\alpha \in \mathcal{P}(E_{/T})$. Let E' be the base change of E along $\mathcal{Q}_{E_{/T}} \to T$ and let $\beta_{\text{univ}} \in \mathcal{Q}(E'_{/\mathcal{Q}_{E_{/T}}})$ be the universal $\mathcal{Q}$-structure. Then there exists a unique map $\mathcal{Q}_{E_{/T}} \to \mathcal{M}(\mathcal{P},\mathcal{Q})$ corresponding to the triple $(E_{/T}, \alpha, \beta_{\text{univ}})$ which is plainly G-equivariant. The composite

$$\mathcal{Q}_{E_{/T}} \to \mathcal{M}(\mathcal{P},\mathcal{Q}) \to \mathcal{M}(\mathcal{P})$$

is G-equivariant, so that we obtain a commutative diagram

$$\begin{array}{ccc} \mathcal{Q}_{E_{/T}} & \xrightarrow{f'} & \mathcal{M}(\mathcal{P},\mathcal{Q}) \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi_{\text{univ}}} \\ T & \xrightarrow{f} & \mathcal{M}(\mathcal{P}). \end{array}$$

We have to check that $(f^*\mathbf{E}, f^*\alpha_{\text{univ}})$ is isomorphic to $(E_{/T}, \alpha)$. We have $\pi^*(f^*\mathbf{E}, f^*\alpha_{\text{univ}}) \simeq (f')^*(\widetilde{\mathbf{E}}, \widetilde{\alpha_{\text{univ}}}, \beta_{\text{univ}})$ which is $(E', \alpha, \beta_{\text{univ}})$ by definition of f'. Consequently we have $\pi^*(f^*\mathbf{E}, f^*\alpha_{\text{univ}}) \simeq \pi^*(E_{/T}, \alpha)$ and this isomorphism commutes to the action of G. By descent, this induces an isomorphism $f^*\mathbf{E} \simeq E$. Now, $\mathcal{P}$ being rigid and π a G-torsor, we have $(f^*\mathbf{E}, f^*\alpha_{\text{univ}}) \simeq (E_{/T}, \alpha)$.

Finally we have to check that f is unique. This is left to the reader who may also consult [KM85]. □

Finally we can prove the representability theorem.

Theorem 6.15. *Let S be a locally noetherian scheme and let $\mathcal{P}$ be some relatively representable affine and rigid moduli problem. Then $\mathcal{P}$ is representable.*

Proof. Assume that we can decompose $S = S' \cup S''$ with S' and S'' open subschemes of S and that there exists $\mathcal{Q}'$ and $\mathcal{Q}''$ representable functors over $\mathcal{E}ll_{S'}$ and $\mathcal{E}ll_{S''}$ satisfying the properties of Lemma 6.14. Then the restrictions $\mathcal{P}|_{S'}$ and $\mathcal{P}_{S''}$ of $\mathcal{P}$ to $\mathcal{E}ll_{S'}$ and $\mathcal{E}ll_{S''}$ are representable by elliptic curves $\mathbf{E}'_{/\mathcal{M}'}$ and $\mathbf{E}''_{/\mathcal{M}''}$. It is now clear that the schemes $\mathcal{M}'$ and $\mathcal{M}''$ can be uniquely glued into an S-scheme $\mathcal{M}$ representing the functor $T \mapsto \{(E_{/T}, \alpha \in \mathcal{P}(E_{/T}))\}/\simeq$. Then the elliptic curves $\mathbf{E}'$ and $\mathbf{E}''$ can be glued into an elliptic curve $\mathbf{E}$ over $\mathcal{M}$ as can be the universal $\mathcal{P}$-structures. The object that we obtain represents the functor $\mathcal{P}$.

We just have to observe that such a decomposition of S can always be obtain. We take $S = S\left[\frac{1}{3}\right]$ and $\mathcal{Q}' = [\Gamma(3)]|_{\mathcal{E}ll_{S'}}$, $S'' = S\left[\frac{1}{2}\right]$ and $\mathcal{Q}'' = [\Gamma(4)]|_{\mathcal{E}ll_{S''}}$. By construction, for each $E_{/T}$, the map $[\Gamma(3)]_{E_{/T}} \to T$ is an étale $\mathrm{GL}_2(\mathbb{F}_3)$-torsor (if $3 \in \Gamma(T, \mathcal{O}_T)^\times$) and $[\Gamma(4)]_{E_{/T}} \to T$ is an étale $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$-torsor (if $2 \in \Gamma(T, \mathcal{O}_T)^\times$). □

Theorem 6.16. *Let $\mathcal{P}$ be some relatively representable finite étale and rigide moduli problem over $\mathcal{E}ll_S$. Then $\mathcal{P}$ is representable by an elliptic curve $\mathbf{E}_{/\mathcal{M}(\mathcal{P})}$ and $\mathcal{M}(\mathcal{P})$ is a smooth and affine curve over S.*

Proof. The assertion is local on the base, so that we can assume that 3 or 2 is invertible. Then $\mathcal{M}(\mathcal{P})$ is isomorphic to $G\backslash\mathcal{M}(\mathcal{P},\mathcal{Q})$ for a well chosen representable functor $\mathcal{Q}$. Actually $\mathcal{M}(\mathcal{P},\mathcal{Q})$ is finite étale over $\mathcal{M}(\mathcal{Q})$. Now we can choose $\mathcal{Q}$ being $\Gamma(3)$ or $\Gamma(4)$ but we checked that $\mathcal{M}(\mathcal{Q})$ is a smooth affine curve over S in both cases. Consequently $\mathcal{M}(\mathcal{P},\mathcal{Q})$ is finite étale over T. Since $\mathcal{M}(\mathcal{P},\mathcal{Q})$ is a G-torsor over $\mathcal{P}$ we can conclude that $\mathcal{M}(\mathcal{P})$ is affine and smooth over S. □

Corollary 6.17. *If $N \geqslant 3$, the moduli problem $[\Gamma(N)]|_{\mathcal{E}ll_{\mathbb{Z}[\frac{1}{N}]}}$ is representable by a smooth and affine curve $\mathcal{M}(\Gamma(N))$ over $\mathbb{Z}[\frac{1}{N}]$. If $N \geqslant 4$, the moduli problem $[\Gamma_1(N)]|_{\mathcal{E}ll_{\mathbb{Z}[\frac{1}{N}]}}$ is representable by a smooth and affine curve $\mathcal{M}(\Gamma_1(N))$ over $\mathbb{Z}[\frac{1}{N}]$.*

6.5 The $\mathbb{C}$-points of moduli spaces of elliptic curves

We constructed a bijection between $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and the set of isomorphism classes of elliptic curves defined over $\mathbb{C}$. The isomorphism sends the orbit of $z \in \mathbb{H}$ to the complex elliptic curve $E_\tau := E_{\Lambda_\tau}$ where $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.

We can construct a level N structure on E_τ depending naturally on τ by the formula

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^2 & \longrightarrow & E_\tau[N] \\ (a,b) & \longmapsto & a\frac{1}{N} + b\frac{\tau}{N}. \end{array}$$

We will now determine to which condition the two pairs

$$\left(E_\tau, \left(\frac{1}{N}, \frac{\tau}{N}\right)\right) \text{ and } \left(E_{\tau'}, \left(\frac{1}{N}, \frac{\tau'}{N}\right)\right)$$

are isomorphic. These pairs are isomorphic if and only if there exists $\alpha \in \mathbb{C}^\times$ such that

$$\begin{cases} \alpha\Lambda_\tau = \Lambda_{\tau'} \\ \frac{\alpha}{N} \in \frac{1}{N} + \Lambda_{\tau'} \\ \frac{\alpha\tau}{N} \in \frac{\tau'}{N} + \Lambda_{\tau'}. \end{cases}$$

This is the case if and only if there exists a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ such that $\tau' = \alpha(a\tau + b)$ and $1 = \alpha(c\tau + d)$ with $\alpha^{-1}\tau' \in \tau + N\Lambda_\tau$ and $\alpha^{-1} \in 1 + N\Lambda_\tau$, ie. the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is actually in $\Gamma(N)$. This proves that the points of $Y(N)$ corresponds to equivalence classes of elliptic curves with full level N structure. However we don't obtain all full level N structures by this process. Namely if $(E, (P, Q))$ is a full level N structure the Weil pairing $e_N(P, Q)$ is invariant by any automorphism of E. As we have

$$e_N\left(\frac{\lambda_1}{N}, \frac{\lambda_2}{N}\right) = \exp\left(\frac{2\pi i}{N}\frac{\mathrm{Im}(\overline{\lambda_1}\lambda_2)}{\mathrm{vol}(\Lambda)}\right)$$

we have $e_N\left(\frac{\tau}{N}, \frac{1}{N}\right) = \exp\left(-\frac{2\pi i}{N}\right)$.

Let $A_N = \mathbb{Z}[1/N, X]/(\Phi_N(X))$ with Φ_N the N-th cyclotomic polynomial. Fix $\zeta \in A_N$ a primitive N-th root. If E/S is an elliptic curve with S an A_N-scheme, define

$$[\Gamma(N)]_\zeta(E/S) = \{(P, Q) \in [\Gamma(N)](E/S),\ e_N(P, Q) = \zeta\}.$$

Then we can easily check that have a bijection

$$Y(N) \simeq \{(E,\alpha),\, \alpha \in [\Gamma(N)]_\zeta(E/S)\}/\sim$$

where $(E,\alpha) \sim (E',\alpha')$ if and only if there is an isomorphism $E \simeq E'$ pulling back α' to α.

Theorem 6.18. *For $N \geqslant 3$, the moduli problem $[\Gamma(N)]_\zeta$ is representable over $\mathcal{E}ll_{A_N}$ by an elliptic curve $\mathcal{E}/\mathcal{M}(\Gamma(N)_\zeta)$ with $\mathcal{M}(\Gamma(N)_\zeta)$ an affine smooth curve over $\operatorname{Spec} A_N$ with geometrically connected fibers. Moreover let ι be the embedding of A_N in $\mathbb{C}$ sending ζ to $e^{\frac{2\pi i}{N}}$, there exists an isomorphism of Riemann surfaces between $Y(N)$ and $(\mathcal{M}(\Gamma(N)_\zeta)\times_\iota \mathbb{C})^{\mathrm{an}}$ given on $\mathbb{C}$-points by*

$$\Gamma(N)\tau \mapsto \left(E_\tau, \left(\frac{1}{N}, \frac{\tau}{N}\right)\right).$$

Proof. The scheme $\operatorname{Spec} A_N$ represents the functor of primitive roots of unity. Consequently there exists a morphism of scheme $\mathcal{M}(\Gamma_N) \to \operatorname{Spec} A_N$ which is defined on the sets on points by $(E,(P_1,P_2)) \mapsto e_N(P_1,P_2)$. The $\operatorname{Spec} A_N$-scheme $\mathcal{M}(\Gamma(N)_\zeta)$ is nothing else than $\mathcal{M}(\Gamma(N))$ viewed as a $\operatorname{Spec} A_N$-scheme via the above map.

We have essentially to prove the existence of the isomorphism between $Y(N)$ and $(\mathcal{M}(\Gamma(N)_\zeta) \times_\iota \mathbb{C})^{\mathrm{an}}$. In order to do that, it is sufficient to construct a morphism of Riemann surfaces

$$\mathcal{M}(\Gamma(N)_\zeta)(\mathbb{C})^{\mathrm{an}} \to Y(\Gamma(N)) \tag{7}$$

which, on $\mathbb{C}$-points is given by (6.18). Namely this will be a bijective morphism between Riemann surfaces, hence an isomorphism because of the complex analytic local inversion theorem.

In order to prove the existence of (7), we use the following result, which is a version "in family" of the complex uniformisation theorem.

Proposition 6.19. *Let S be a smooth $\mathbb{C}$-scheme and let E be some elliptic curve over S. Then there exists a line bundle $\mathcal{V}$ on S, a rank 2 local system Λ on S^{an}, a map of sheaves $\Lambda \hookrightarrow \mathcal{V}^{\mathrm{an}}$ and a holomorphic map $\mathbb{V}(\mathcal{V}^{\vee,\mathrm{an}}) \to E^{\mathrm{an}}$ inducing, for all $s \in S(\mathbb{C})$,*

$$\mathcal{V} \otimes k(s)/\Lambda_s \simeq E_s.$$

Such a pair is called an uniformisation of E^{an}.

Let $(\Lambda \hookrightarrow \mathcal{V})$ be some uniformisation of E^{an} as in the Proposition. Locally on S^{an} (for the analytic topology), the sheaf Λ is isomorphic to $\mathbb{Z}^2$. Up to localising on S, we can fix an isomorphism of local systems $\mathbb{Z}^2 \simeq \Lambda$. The map $\Lambda \hookrightarrow \mathcal{V}$ induces a morphisme of vector bundles

$$\Lambda \otimes \mathcal{O}_S \twoheadrightarrow \mathcal{V}.$$

The map is surjective since, for each point $s \in S(\mathbb{C})$, the image of Λ_s in $\mathcal{V}\otimes k(s)$ contains a basis. Now if we fix an isomorphism $\psi : \mathbb{Z}^2 \simeq \Lambda$, we obtain a surjective map of vector

bundles $\mathcal{O}_S^2 \twoheadrightarrow \mathcal{V}$ with $\mathcal{V}$ a line bundle. This is equivalent to a map $S \to \mathbb{P}^1_{\mathbb{C}}$. Moreover, for $s \in S(\mathbb{C})$, we know that Λ_s contains a basis of the $\mathbb{R}$-vector space $\mathcal{V} \otimes k(s)$. This implies that the map $S(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ takes its values in $\mathbb{P}^1(\mathbb{C}) \setminus \mathbb{P}^1(\mathbb{R})$, identified to $\mathbb{C} \setminus \mathbb{R}$ via $x \mapsto (x:1)$. Moreover it is easily checked that the map $S^{\mathrm{an}} \to \mathbb{C} \setminus \mathbb{R}$ is holomorphic. Namely there is an holomorphic section h of $\mathcal{V}$ such that $\psi((0,1)) = h\psi((1,0))$ so that the map $s \mapsto h(s)$ is holomorphic. Obviously the map $S^{\mathrm{an}} \to \mathbb{C} \setminus \mathbb{R}$ depends on the choice of the trivialisation ψ. Namely if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, then $\psi \circ \gamma^{-1}$ is another trivialisation and $h(\psi \circ \gamma^{-1}) = \frac{ah(\psi)+b}{ch(\psi)+d}$. As a consequence, we can always choose ψ so that the map $h(\psi)$ takes its values in $\mathbb{H} \subset \mathbb{C} \setminus \mathbb{R}$.

If we apply the snake Lemma to the morphism of sheaves over S^{an} :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathcal{V} & \longrightarrow & E & \longrightarrow & 0 \\ & & \downarrow N & & \downarrow N & & \downarrow N & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathcal{V} & \longrightarrow & E & \longrightarrow & 0 \end{array}$$

we obtain an isomorphism of local systems

$$\Lambda \otimes \mathbb{Z}/N\mathbb{Z} \simeq E[N]. \tag{8}$$

Now assume that we have a full level N structure on E, ie an isomorphism $(\mathbb{Z}/N\mathbb{Z})^2 \simeq E[N]$, we can consider trivialisation ψ such that (8) induces the isomorphism coming from the level structure. Note that the existence of such a trivialisation comes from our condition $e_N(P,Q) = \zeta$ on the level structure. Two such trivialisations differ by composition with an element of $\Gamma(N)$. Consequently the holomorphic map $S^{\mathrm{an}} \to Y(N) = \Gamma(N)\backslash\mathbb{H}$ that we obtain does not depend on the trivialisation of Λ (compatible with the level structure). Such a construction is local on S, but by uniqueness it can be glued into an holomorphic map $S^{\mathrm{an}} \to Y(N)$. It is a simple exercice (left to the reader) to check that this is exactly the desired map on the points. □

Proof of the Proposition (sketch). We define $\mathcal{V} \coloneqq R^1 f_* \mathcal{O}_E$. Note that $\mathcal{V}$ is a line bundle whose formation commutes with base change. We define $\Lambda \coloneqq R^1 f_* \mathbb{Z}$. It follows from Ehresmann Theorem that $R^1 f_* \mathbb{Z}$ is a local system on S^{an} whose formation commutes with base change. It is sufficient to compute his rank when S is a point and E is a complex torus. This shows that $R^1 f_* \mathbb{Z}$ is a local system of rank 2. Now the short exact sequence on E^{an} :

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_E \xrightarrow{\exp(2\pi i \cdot)} \mathcal{O}_E^\times \longrightarrow 0$$

shows that we have a long exact sequence

$$0 \longrightarrow \Lambda \longrightarrow \mathcal{V} \longrightarrow R^1 f_* \mathcal{O}_E^\times \longrightarrow R^2 f_* \mathbb{Z} \longrightarrow 0.$$

As the sheaf $R^1 f_* \mathcal{O}_E^\times$ is isomorphic to the Picard group $\mathrm{Pic}_{E/S}$ and since the kernel of deg is divisible, we conclude that we obtain a short exact sequence

$$0 \longrightarrow \Lambda \longrightarrow \mathcal{V} \longrightarrow \mathrm{Pic}^0_{E/S} \longrightarrow 0.$$

Now we can use the Abel-Jacobi isomorphism $E \simeq \mathrm{Pic}^0_{E/S}$ in order to obtain the desired map $\mathbb{V}(\mathcal{V}^\vee) \to E^{\mathrm{an}}$. □

There is an analogous result for the moduli problem $[\Gamma_1(N)]$ but, in this case, the moduli space is defined over $\mathbb{Z}[1/N]$.

Theorem 6.20. *For $N \geqslant 4$, the moduli problem $[\Gamma_1(N)]$ is representable over $\mathcal{E}ll_{\mathbb{Z}[1/N]}$ by an elliptic curve $\mathcal{E}/\mathcal{M}(\Gamma_1(N))$ with $\mathcal{M}(\Gamma_1(N))$ an affine smooth curve over $\operatorname{Spec}\mathbb{Z}[1/N]$ with geometrically connected fibers. Moreover there exists an isomorphism of algebraic varieties over $\mathbb{C}$ between $Y_{\Gamma_1(N)}$ and $\mathcal{M}(\Gamma(N)_\zeta) \times \mathbb{C}$ given on $\mathbb{C}$-points by*

$$\Gamma(N)\tau \mapsto \left(E_\tau, \frac{1}{N}\right).$$

6.6 Coarse moduli schemes

Let S be a scheme and let $\mathcal{P}$ be some moduli problem over $\mathcal{E}ll_S$ which is relatively representable and affine. We construct a *coarse moduli scheme* for $\mathcal{P}$ by the following process. Locally on S, we define

$$M(\mathcal{P}) \coloneqq G\backslash\mathcal{M}(\mathcal{P}, \mathcal{Q})$$

where $\mathcal{Q}$ is a representable moduli problem which is moreover a finite étale torsor of group G. We can check that this definition does not depend on the choice of the functor $\mathcal{Q}$, it is unique up to unique isomorphism so that it can be defined locally and glued over S.

Proposition 6.21. *Let $S = \operatorname{Spec}\mathbb{Z}[1/N]$ and assume that $\mathcal{P}$ is moreover finite étale and surjective. Then $M(\mathcal{P})$ is normal and finite flat over S, of relative dimension 1.*

Proof. All these assertions are local on the base. We can consequently assume that $M(\mathcal{P}) = G\backslash\mathcal{M}(\mathcal{P}, \mathcal{Q})$. We have a commutative diagram

$$\begin{array}{ccc} \mathcal{M}(\mathcal{P}, \mathcal{Q}) & \longrightarrow & M(\mathcal{P}) \\ \downarrow & \searrow & \downarrow \\ \mathcal{M}(\mathcal{Q}) & \longrightarrow & S \end{array}$$

We know that the horizontal bottom arrow is smooth and affine and the left vertical arrow is finite étale and surjective. Then the diagonal arrow is smooth and affine. As the top horizontal arrow is a quotient by a finite group, we can conclude that $M(\mathcal{P})$ is normal and torsion free over S, consequently S-flat. The finiteness is a consequence of the fact that $\mathcal{M}(\mathcal{P}, \mathcal{Q})$ is finite over S and that S is noetherian. □

More general moduli problems Let $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be some subgroup. We define the H-structure moduli problem. Let $E_{/S}$ be some elliptic curve with N invertible over S. The moduli problem $[\Gamma(N)]$ is relatively representable we can consider the S-scheme $[\Gamma(N)]_{E_{/S}}$ which is smooth and finite étale over S. The finite group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $[\Gamma(N)]$ and consequently acts on $[\Gamma(N)]_{E_{/S}}$. Thus we can define set

$$[H](E_{/S}) \coloneqq \mathrm{Hom}_S(S, H\backslash[\Gamma(N)]_{E_{/S}}).$$

The functor $[H]$ is a moduli problem which is relatively representable and finite étale over $\mathcal{E}ll_{\mathbb{Z}[1/N]}$. Assume that S is connected and locally noetherian and fix $\overline{s}$ some geometric point of S. We can give the following interpretation of the elements of $[H](E_{/S})$: they are the H-orbits (on the left) of group isomorphisms

$$(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]_{\overline{s}}$$

which are stable under the action of the fundamental group $\pi_1(S, \overline{s})$ (on the right).

Using this description we can check that the moduli problem $[\Gamma_0(N)]$ is isomorphic to $[H]$ with H the subgroup of upper triangular matrices and $[\Gamma_1(N)]$ corresponds to the subgroup of upper triangular matrices with upper left entry equal to 1.

As the formation of quotients commutes to flat base change and the map $\mathrm{Spec}\,\mathbb{C} \to \mathrm{Spec}\,\mathbb{Z}[1/N]$ is flat, we have natural isomorphism of Riemann surfaces

$$H\backslash\mathcal{M}(\Gamma(N))(\mathbb{C}) \xrightarrow{\sim} M(H)(\mathbb{C})$$

which induces an isomorphism

$$X_{K_H} \xrightarrow{\sim} M(H)(\mathbb{C})$$

with K_H the compact open subgroup $K_H \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ defined as the inverse image of H by the reduction map

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

The classifying map Let $\mathcal{P}$ be a relatively representable and affine moduli problem over $\mathcal{E}ll_S$. Each isomorphism class $(E_{/T}, \alpha)$ with $\alpha \in \mathcal{P}(E_{/T})$ gives rise to a *classifying map*

$$T \longrightarrow M(\mathcal{P})$$

that is a morphism of S-schemes defined locally on T as follows. As usual we fix $\mathcal{Q}$ some representable moduli problem which is an étale G-torsor for some finite group G. We consider the universal $\mathcal{Q}$-structure over $E_{/\mathcal{Q}_{E_{/T}}}$ giving rise to a map $\mathcal{Q}_{E_{/T}} \to \mathcal{M}(\mathcal{P}, \mathcal{Q})$. Since $\mathcal{Q}$ is a finite étale G-torsor, the G-equivariant map $\mathcal{Q}_{E_{/T}} \to T$ is a quotient, so that the following diagram can be completed

$$\begin{array}{ccc} \mathcal{Q}_{E_{/T}} & \longrightarrow & \mathcal{M}(\mathcal{P}, \mathcal{Q}) \\ \downarrow & & \downarrow \\ T & \dashrightarrow & M(\mathcal{P}) \end{array}$$

The bottom horizontal map is then the classifiying map.

Consequently each pair $(E_{/T}, \alpha)$ gives rise to a canonical T-point of $x_{E_{/T},\alpha} \in M(\mathcal{P})(T)$.

Proposition 6.22. *Let k be some algebraically closed field. The map $(E_{/k}, \alpha) \mapsto x_{E_{/T},\alpha}$ induces a bijection from the set of isomorphism classes of pairs $(E_{/k}, \alpha)$ and the set $M(\mathcal{P})(k)$.*

Proof. It follows from properties of quotient of schemes by finite groups that we are reduced to check that the set of isomorphism classes of pairs $(E_{/k}, \alpha)$ are in bijection with the orbits of G on k-points of $\mathcal{M}(\mathcal{P}, \mathcal{Q})$. As $\mathcal{P} \times \mathcal{Q}$ is representable, the k-points of $\mathcal{M}(\mathcal{P}, \mathcal{Q})$ are in bijection with isomorphism classes of triples $(E_{/k}, \alpha, \beta)$ with β some $\mathcal{Q}$-structure on $E_{/k}$. The conclusion comes from the fact that, $\mathcal{Q}$ being a G-torsor, the group G acts transitively on triples $(E_{/k}, \alpha, \beta)$ with fixed isomorphism class $(E_{/k}, \alpha)$. □

6.7 The j-line

The discriminant Recall that we defined $\widetilde{S} = \operatorname{Spec} \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ the scheme of parameters of Weierstrass equations and S^{univ} the open subscheme of smooth equations. We recall that there is a universal projective curve $\widetilde{E}$ over $\widetilde{S}$ defined by the projective equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Proposition 6.23. *Up to sign, there exists a unique $\Delta \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ such that $\widetilde{S} \smallsetminus S^{\text{univ}} = \{\Delta = 0\}$.*

Proof. Let $\widetilde{E}^{\text{sm}}$ be the smooth locus of $f : \widetilde{E} \to \widetilde{S}$. We have to check that the closed subspace $f(\widetilde{E} \smallsetminus \widetilde{E}^{\text{sm}})$ is of pure codimension 1. The conclusion follows then from the fact that $\widetilde{S}$ is the spectrum of a factorial ring. However $\widetilde{E} \smallsetminus \widetilde{E}^{\text{sm}}$ is defined by three equations in $\mathbb{P}^2_{\widetilde{S}}$, its irreducible components are consequently of codimension $\leqslant 3$. As all fibers of f contains smooth points, we deduce that the irreducible components of $\widetilde{E} \smallsetminus \widetilde{E}^{\text{sm}}$ have codimension $\leqslant 2$. As f is flat and has generically smooth fibers, we conclude that irreducible components of $f(\widetilde{E} \smallsetminus \widetilde{E}^{\text{sm}})$ have codimension $\leqslant 1$. Finally, $\widetilde{S}$ being irreducible and S^{univ} non empty, the closed subset $S \smallsetminus S^{\text{univ}}$ is of pure dimension 1. □

This Δ is called the *discriminant* and can be calculated explicitely as follows.

Define

$$\begin{cases} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6. \end{cases}$$

Over $\widetilde{S}[1/2]$, there is a isomorphism of projective curves

$$\operatorname{Proj} \mathcal{O}_{\widetilde{S}[1/2]}[x_1, y_1, z_1]/(y_1^2z_1 = 4x_1^3 + b_2x_1^2z_1 + 2b_4x_1z_1^2 + b_6z_1^3) \xrightarrow{\sim} \widetilde{E}$$

given by $(x : y : z) \mapsto (x_1 : y_1 : z_1) = (x : 2y + a_1x + a_3z : z)$.

By unicity, we conclude that Δ must be a $\mathbb{Z}[1/2]^\times$ multiple of the discriminant of the polynomial

$$x^3 + b_2x^2 + 2b_4x + b_6.$$

Up to ± 1, we find that there exists a unique such multiple which is non zero on $\widetilde{S} \otimes_{\mathbb{Z}} \mathbb{F}_2$. It is

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where $b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$ (see [Tat74, §2] or [Sil86, III.]).

Moreover if we set $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$, then we have an isomorphism over $\widetilde{S}[1/6]$:

$$\operatorname{Proj} \mathcal{O}_{\widetilde{S}[1/2]}[x_2, y_2, z_2]/(y_2^2z_2 = x_2^3 - 27c_4x_2z_2^2 - 54c_6z_2^3) \xrightarrow{\sim} \widetilde{E}.$$

We define the *j-invariant* as a regular function over S^{univ} by the formula

$$j = \frac{c_4}{\Delta}.$$

Proposition 6.24. *Let T be a scheme and let π_1 and π_2 be two morphisms $T \to S^{\text{univ}}$ such that $\pi_1^*E^{\text{univ}} \simeq \pi_2^*E^{\text{univ}}$, then we have $j \circ \pi_1 = j \circ \pi_2$.*

Proof. This is a consequence of Riemann-Roch Theorem and the formula of change of variable from [Tat74, p. 181]. □

This implies that for each elliptic curve $E_{/T}$, there exists a unique morphism $j : T \to \mathbb{A}^1$ such that, if $U \subset T$ is an open subset such that $E_{/U}$ is obtained by pullback from some $\pi : U \to S^{\text{univ}}$, then $j|_U = j \circ \pi$. A consequence of the unicity is that, if f is automorphism of $E_{/T}$, we have $j \circ f = j$. This implies that j factors through a morphism

$$j : M(1) \to \mathbb{A}^1_{\mathbb{Z}}.$$

Theorem 6.25. *Assume that k is an algebraically closed field, then j induces a bijection*

$$M(1)(k) \xrightarrow{\sim} k.$$

Proof. See for example [Sil86, Prop. III.1.4]. □

Theorem 6.26. *The map j induces an isomorphism of schemes*

$$j : M(1) \xrightarrow{\sim} \mathbb{A}^1_{\mathbb{Z}}.$$

Proof. The scheme $M(1)$ is normal and flat over $\mathbb{Z}$. As $\mathcal{M}(\Gamma(3)) \to M(1)$ is finite and surjective, the scheme $M(1)$ has to be of dimension 2. Consequently Serre normality criterion ([Gro65, Thm. 5.8.6]) implies that $M(1)$ is Cohen-Macaulay. It follows from Theorem 6.25 that the map j is quasi-finite. A quasi-finite map between two schemes of same dimension, the source being Cohen-Macaulay and the target a regular scheme, is flat. Consequently j is finite flat. Looking at complex points, we see that j has degree 1 on a dense subset of $M(H)$. Consequently j is a finite flat morphism of degree 1, hence an isomorphism, from $M(H)$ to its image in $M(1)$. As Theorem 6.25 shows that j is surjective on closed points and both schemes are finitely generated over $\mathbb{Z}$, j is surjective and consequently an isomorphism. □

This implies that the coarse moduli scheme $M(1)$ is affine and smooth over $\operatorname{Spec}\mathbb{Z}$.

More generally we have the following result :

Theorem 6.27. *Let $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup. Then the coarse moduli problem $M(H)$ is affine and smooth over $\operatorname{Spec}\mathbb{Z}[1/N]$ of relative dimension 1. Moreover if $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, then its geometric fibers are connected.*

Proof. See [DR73, Prop. 6.7]. □

6.8 Compactification of moduli problems

The goal of this section is to "compactify" the modular curves $M(H)$ as we compactified their complex analytic analogues $X(H)$.

The coarse moduli scheme $M(1)$ is an open subscheme of a proper and smooth scheme over $\operatorname{Spec}\mathbb{Z}$. Namely it is isomorphic to $\mathbb{A}^1_{\mathbb{Z}}$ through j and $\mathbb{A}^1_{\mathbb{Z}}$ can be compactified by $\mathbb{P}^1_{\mathbb{Z}}$.

Let $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup. We define a scheme $\overline{M(H)}$ as the normalisation of $\mathbb{P}^1_{\mathbb{Z}[N^{-1}]}$ into $M(H)$ via the finite map

$$f : M(H) \to M(1).$$

More precisely let $U \subset \mathbb{P}^1_{\mathbb{Z}[N^{-1}]}$ be some affine open subset and let $U' = U \cap \mathbb{A}^1_{\mathbb{Z}[N^{-1}]}$ and $V' = f^{-1}(U')$. Let $U = \operatorname{Spec} A$. The map f being finite, V' is an open affine subset of $M(H)$. Let B be the integral closure of A in $\mathcal{O}(V')$ which is finite extension of $\mathcal{O}(U')$. The ring B is a finite A-module. Namely, we know that $\mathbb{Z}$ is an universally japanese ring (by [Gro65, Cor. 7.7.4]) which means that if A is a finitely generated $\mathbb{Z}$-algebra which is a domain and if K' is a finite extension of the fraction field K of A, then the integral closure of A in K' is a finite A-module (see [Gro64, §23] for more details). Here A is clearly a finitely generated $\mathbb{Z}$-algebra. Since $M(H)$ is a normal scheme, the ring B can be described as the integral closure of A in the fraction ring of $\mathcal{O}(V')$ which is a finite sum of finite extension of $\operatorname{Frac} A$. Consequently we can define $V \coloneqq \operatorname{Spec} B$. It is a normal

scheme and the map $V \to U$ is finite. We can remark that all the connected components of $\operatorname{Spec} B$ are normal schemes of dimension 2. Consequently they are Cohen-Macaulay and $\operatorname{Spec} B$ is Cohen-Macaulay. The map $\operatorname{Spec} B \to \operatorname{Spec} A$ is consequently a finite map between equidimensional schemes of the same dimension, with A regular and B Cohen-Macaulay. Thus B is flat A-module.

From the normality of $M(H)$, we deduce that, $U = U'$ implies $V = V'$. This implies that, if (U_i) is finite open affine covering of $M(1)$, we obtain a family (V_i) of affine schemes which can be glued into a normal scheme $\overline{M(H)}$ with a finite flat map

$$\overline{M(H)} \to \overline{M(1)}$$

and there exists a natural open embedding $M(H) \hookrightarrow \overline{M(H)}$ inducing an isomorphism

$$M(H) \simeq \overline{M(H)} \times_{\overline{M(1)}} M(1).$$

Note that $\overline{M(1)}$ is proper, so that $\overline{M(H)}$ is a proper $\mathbb{Z}$-scheme. It deserves to be thought as the "compactification" of $M(H)$.

Remark 6.28. The scheme $M(H)$ has a moduli interpretation as a (coarse) moduli space parametrising elliptic curves with additional structure. We can give a similar moduli interpretation of the $\overline{M(H)}$. However we have to work not only with elliptic curve but with *generalised elliptic curve* making the theory more technical. However this description can be very useful if we want to describe the singularities appearing when we normalise $M(H)$ over $\operatorname{Spec} \mathbb{Z}$ (and not only $\operatorname{Spec} \mathbb{Z}[N^{-1}]$. The interested readers can have a look to [DR73].

It is a bit more complicated that this process gives us a smooth curve.

Theorem 6.29. *The $\mathbb{Z}[1/N]$-scheme $\overline{M(H)}$ is proper and smooth over $\operatorname{Spec} \mathbb{Z}[1/N]$.*

Before proving this theorem, let's introduce the *cuspidal divisor*. This is the closed subscheme $\operatorname{Cusp}_H := (\overline{M(H)} \smallsetminus M(H))^{\mathrm{red}}$. Since $M(H)$ is a norma scheme, Cusp_H coincide with the inverse image of $\infty := \overline{M(1)} \smallsetminus M(1)$ which is isomorphic to $\operatorname{Spec} \mathbb{Z}$. This proves that Cusp_H is a finite flat $\mathbb{Z}$-scheme. This is an effective divisor in $\overline{M(H)}$.

Proposition 6.30. *The divisor Cusp_H is a disjoint union of irreducible divisors.*

Proof. Namely let $U = \operatorname{Spec} A$ be some affine open subset of $\overline{M(1)}$ containing ∞. Then Cusp_H is contained in the inverse image of U which is the normalisation of A in the fraction ring of $\mathcal{O}(V')$ where V' is the inverse image of $U' = U \cap M(1)$ in $M(H)$. The fraction ring of $\mathcal{O}(V')$ is finite sum of fields and B is consequently the finite sum of the normalisation of A in each of these fields. This proves the assertion. □

Theorem 6.29 can be deduced from a variant ofAbhyankar Lemma ([SGA03, Prop. XIII.5.2]).

Let X be a normal scheme and let $D \subset X$ be an irreducible regular closed subscheme of codimension 1. Let $U = X \smallsetminus D$ and let $f : V \to U$ be some finite étale morphism. We say that f is tamely ramified along D if, for $x \in D$ the generic point, η a generization of x in U and η' a generic point of V such that $f(\eta') = \eta$, the extension $k(\eta')/k(\eta)$ is tamely ramified over the discrete valuation ring $\mathcal{O}_{X,x} \subset k(\eta)$. In other word, the inertia index of all primes of $k(\eta)$ over x are prime to the characteristic of the residue field $k(x)$.

Theorem 6.31. *Let X be a regular scheme and let $D \subset X$ an irreducible regular closed subscheme of codimension 1. Let $f : Y \to X$ be finite flat morphism which is étale over $X \smallsetminus D$ with Y normal and f tamely ramified along D. Then the ramification index e of f along D is prime to the characteristic of all closed points of D. Moreover there exists an étale map $h : X' \to X$ whose image contains D, an element $x \in \Gamma(X', \mathcal{O}_{X'})$ such that $h^{-1}(D) = \{x = 0\}$ such that $Y \times_X X'$ is isomorphic to $\operatorname{Spec} \mathcal{O}_{X'}[T]/(T^e - x) \to \operatorname{Spec} X'$.*

Proof. See [Con, Lemm. 1.4+Erratum]. □

Proof of Theorem 6.29. We can apply Theorem 6.31 if we know that there exists some open subset U of $\overline{M(1)}$ such that the map $\overline{M(H)} \to \overline{M(1)}$ is étale on $U \smallsetminus \mathrm{Cusp}$. It is therefore sufficient to check that the map $M(H) \to M(1)$ is finite étale on some open subset of $M(1)$ complement of a finite union of closed subsets of the form $\{j = a\}$ for $a \in \mathbb{Z}$. The map $M(H) \to M(1)$ is finite étale of degree $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : H\{\pm 1\}]$. Consequently it is finite étale at a geometric point $x : \operatorname{Spec} k \to M(1)$ if and only if its fiber has exactly d_H points over x. This is the case if and only if $\mathrm{Aut}(E_x) = \{\pm I_2\}$. It can be checked on Weierstrass equations that this is true as soon as $j(E_x) \notin \{0, 1728\}$. Consequently the map $M(H) \to M(1)$ is étale outside of $\{j = 0\} \cup \{j = 1728\}$. Then Theorem 6.31 implies that there exists some étale map $\operatorname{Spec} A = X' \to \overline{M(1)}$ whose image contains ∞ and such that $X' \times_{\overline{M(1)}} \overline{M(H)}$ is isomorphic to $A[X]/(X^e - x)$ for some $x \in A$. As e is prime to the residual characteristic of all the points of Cusp_H, we deduce that $A[X]/(X^e - x)$ is a finite étale A-algebra. It follows that the map $\overline{M(H)} \to \overline{M(1)}$ is étale on the neighbourhood of Cusp_H and consequently that $\overline{M(H)}$ is a smooth $\mathbb{Z}[N^{-1}]$-scheme. □

Example 6.32. If $p \in \{11, 17, 19\}$, the scheme $\overline{M(\Gamma_0(p))}_{\mathbb{Q}}$ is an elliptic curve having good reduction outside of p.

For example, $\overline{M(\Gamma_0(11))}$ is the projective scheme over $\mathbb{Z}[11^{-1}]$ defined by

$$y^2z + yz^2 = x^3 - x^2z - 10xz^2 - 20z^3. \tag{9}$$

Namely, it is an equation defining $\overline{M(\Gamma_0(11))}_{\mathbb{C}} \simeq X_0(11)$. Moreover the discriminant of this Weierstrass equation is -11^5, so that it defines a proper and smooth scheme over $\mathbb{Z}[11^{-1}]$ which has to coincide with $\overline{M_0(11)}$.

Note that this equation defines a projective scheme over $\mathbb{Z}$ which is normal. However this scheme is not smooth over $\mathbb{Z}$. Namely its fiber at 11 is the curve define by the equation

$$(y - 5z)^2 = (x - 5z)^3 + 3(x - 5z)^2.$$

It has a singular point at $(5:5:1)$. Moreover we can check that the scheme defined by (9) is not regular at this point.

Similarly the scheme $\overline{M(\Gamma_1(11))}$ is an elliptic curve over $\mathbb{Z}[11^{-1}]$ defined by the equation

$$y^2z + yz^2 = x^3 - x^2z. \tag{10}$$

The same equation defines a normal projective scheme over $\mathbb{Z}$. It has a singular fiber at 11 of singular point $(-3:5:1)$. This time the equation (10) defines a regular scheme in $\mathbb{P}^2_{\mathbb{Z}}$ (even if is not smooth over $\operatorname{Spec}\mathbb{Z}$).

7 A geometric description of Hecke operators (in weight 2)

7.1 Cohomology of compact Riemann surfaces

Let X be some compact Riemann surface. Let $\Omega(X)$ be the finite dimensional $\mathbb{C}$-vector space of holomorphic differential on X and let $H^1(X,\mathbb{Z})$ be the first cohomology group of X and $H_1(X,\mathbb{Z})$ its first homology group. These two groups are finite free of rank $g = g(X)$ and there is a natural group isomorphism $H^1(X,\mathbb{Z}) \simeq \operatorname{Hom}(H_1(X),\mathbb{Z})$. By integration, we can define a group homomorphism

$$H_1(X) \longrightarrow \Omega(X)' \coloneqq \operatorname{Hom}_{\mathbb{C}}(\Omega(X),\mathbb{C}).$$

Namely if $\gamma : [0,1] \to X$ is a differential map, we can define the integral $\int_\gamma \omega$ of a differential form ω on γ. As holomorphic forms are closed, we have $\int_{\gamma_1}\omega = \int_{\gamma_2}\omega$ if γ_1 and γ_2 are two homotopic paths in X (see for example [FK80, §I.4]). Consequently the map $\gamma \mapsto \int_\gamma$ induces a group homomorphism from $\pi_1(X)$ to $\Omega(X)'$. As $H_1(X,\mathbb{Z})$ is canonically isomorphic to the abelianization of $\pi_1(X)$, we obtain the desired map $H_1(X) \to \Omega(X)'$.

We will admit without proof that this map induces an isomorphism

$$H_1(X,\mathbb{R}) \simeq H_1(X,\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} \Omega(X)'.$$

(for a proof see [FK80, §III.2] but treating directly the case of X a complex elliptic curve via complex uniformisation can be instructive.)

By duality, we deduce an injection of $\mathbb{C}$-vector spaces

$$\Omega(X) \hookrightarrow H^1(X,\mathbb{C}) \simeq H^1(X,\mathbb{Z})$$

and a decomposition $H^1(X,\mathbb{C}) = \Omega(X) \oplus \overline{\Omega(X)}$ where $z \mapsto \overline{z}$ is the map defined by $\sum c_i \otimes z_i \mapsto \sum c_i \otimes \overline{z_i}$ on $H^1(X,\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$.

7.2 Hecke operators

Let Γ be some congruence subgroup and recall that we have an isomorphism of $\mathbb{C}$-vector spaces $S_2(\Gamma) \simeq \Omega(X(\Gamma))$. We want to give a geometric description of Hecke operators on $\Omega(X(\Gamma))$.

If $\Gamma' \subset \Gamma$, then the map $\pi : X(\Gamma') \to X(\Gamma)$ is a ramified covering of Riemann surfaces. If ω is an holomorphic form on $X(\Gamma')$, we can define an holomorphic form $\operatorname{Tr}\pi(\omega)$ on $X(\Gamma)$ as follows.

- If π is étale, we use the fact that, for some sufficiently small open subset U in $X(\Gamma)$, $\pi^{-1}(U)$ is a disjoint union $U_1 \cup \cdots \cup U_n$ of open subset of $X(\Gamma')$ isomorphic to U, and we define $\operatorname{Tr}\pi(\omega) = \sum_i (\pi^*\omega)|_{U_i}$ where we identify U_i to U via $\pi|_{U_i}$.
- In the general case, let $Y \subset X(\Gamma)$ be the open subset over which π is étale and let $\pi' = \pi|_{\pi^{-1}(Y)}$. Then we can consider the differential form $\operatorname{Tr}\pi'(\omega|_{\pi^{-1}(Y)})$. A local computation (around ramification points of π) shows that it extends uniquely to an holomorphic form on $X(\Gamma)$.

We obtain a map of complex vector spaces $\Omega(X(\Gamma')) \to \Omega(X(\Gamma))$.

Now we focus on the case where $\Gamma = \Gamma_1(N)$. Let p be a prime number and let $\alpha_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. There is a map of Riemann surfaces $X(\alpha_p\Gamma_1(N)\alpha_p^{-1}) \to X(\Gamma_1(N))$ induced by the action of α_p on $\mathbb{H}$. This gives rise to a map

$$\alpha_p : X(\Gamma_1(N) \cap \alpha_p\Gamma_1(N)\alpha_p^{-1}) \to X(\Gamma_1(N)).$$

If ω is an holomorphic differential on $X(\Gamma_1(N))$, we can "pull" ω on $X(\Gamma_1(N)\cap\alpha_p\Gamma_1(N)\alpha_p^{-1})$ in order to obtain an holomorphic differential $\alpha_p^*\omega$ on $X(\Gamma_1(N) \cap \alpha_p\Gamma_1(N)\alpha_p^{-1})$ and "push" this holomorphic differential on $X(\Gamma)$ via $\operatorname{Tr}\pi$ where $\pi : X(\Gamma_1(N)\cap\alpha_p\Gamma_1(N)\alpha_p^{-1}) \to X(\Gamma_1(N))$ induced by the inclusion of $\Gamma_1(N) \cap \alpha_p\Gamma_1(N)\alpha_p^{-1}$ in $\Gamma_1(N)$. We obtain a new holomorphic differential on $X(\Gamma)$ which is the image of ω via the Hecke operator T_p. It is important to note that we use two maps from $X(\Gamma_1(N) \cap \alpha_p\Gamma_1(N)\alpha_p^{-1})$ to $X(\Gamma_1(N))$:

$$\begin{array}{ccc} & X(\Gamma_1(N) \cap \alpha_p\Gamma_1(N)\alpha_p^{-1}) & \\ {\scriptstyle\pi}\swarrow & & \searrow{\scriptstyle\alpha_p} \\ X(\Gamma_1(N)) & & X(\Gamma_1(N)) \end{array} \tag{11}$$

Now it is a simple computation to check that the following diagram is commutative

$$\begin{array}{ccc} \Omega(X(\Gamma_1(N))) & \xrightarrow{\alpha_p^*} & \Omega(X(\Gamma_1(N) \cap \alpha_p\Gamma_1(N)\alpha_p^{-1})) \\ & {\scriptstyle T_p}\searrow & \downarrow{\scriptstyle \operatorname{Tr}\pi} \\ & & \Omega(X(\Gamma_1(N))) \end{array}$$

Namely assume that ω comes from the holomorphic differential $f(z)\,\mathrm{d}z$ on $\mathbb{H}$ with $f \in S_2(\Gamma_1(N))$. Then $\operatorname{Tr}\pi\alpha_p^*(\omega)$ corresponds to

$$\sum_{g\in(\Gamma_1(N)\cap\alpha_p\Gamma_1(N)\alpha_p^{-1})\backslash\Gamma_1(N)} g^*\alpha_p^*(f(z)\,\mathrm{d}z).$$

However if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})_+$, we have $\gamma^*(f(z)\,\mathrm{d}z) = f(\frac{az+b}{cz+d}\frac{ad-bc}{(cz+d)^2}\,\mathrm{d}z = f[\gamma]_2(z)\,\mathrm{d}z$. This implies the result.

Proposition 7.1. *The lattice $H^1(X(\Gamma_1(N)),\mathbb{Z})$ inside $\Omega(X(\Gamma_1(N)))$ is stable under the action of T_p.*

Proof. It is sufficient to prove that if $\pi : X' \to X$ is a map between two compact Riemann surfaces we can define to morphisms $\pi^* : H^1(X,\mathbb{Z}) \to H^1(X',\mathbb{Z})$ and $H^1(X',\mathbb{Z}) \to H^1(X,\mathbb{Z})$ which are compatible with the inclusion $H^1(X,\mathbb{Z}) \hookrightarrow \Omega^1(X)$ and with π^* and $\operatorname{Tr}\pi$ on differential forms. The map π^* is just the contravariance of the cohomology. We can define π_* using the covariance of the cohomology with compact support and, since X is compact, that $H^1(X,\mathbb{Z}) = H^1_c(X,\mathbb{Z})$. The compatibility of π^* with $H^1(X,\mathbb{Z}) \hookrightarrow \Omega^1(X)$ is easy. The compatibility of π_* is a bit more painful to check, we will admit it. □

We can finally give a proof of Theorem 3.39 in weight 2.

Corollary 7.2. *In $S_2(\Gamma_1(N))$, there is a lattice stable under $\mathcal{H}_2(N)_\mathbb{Z}$.*

Proof. The algebra $\mathcal{H}_2(N)_\mathbb{Z}$ is generated by the operators T_p and $T(p,p)$ for p a prime number and by the diamond operators $\langle d\rangle$ for d prime to N. We take $H^1(X(\Gamma_1(N)),\mathbb{Z})$ as a lattice. The stability under T_p is a consequence of Proposition 7.1. The stability under $T(p,p)$ and $\langle d\rangle$ is easier. Namely the operators $T(p,p)$ and $\langle d\rangle$ on $\Omega(X(\Gamma_1(N)))$ coincide with the pull back by the matrices $\left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$ and $g_d \in \Gamma_0(N)$ where g_d is reduced to $\left(\begin{smallmatrix} d^{-1} & * \\ 0 & d \end{smallmatrix}\right)$ modulo N (these both matrices normalise $\Gamma_1(N)$). □

From Corollary 7.2, we know that, for an eigensystem $\psi : \mathcal{H}_2(N)_\mathbb{Q} \to \overline{\mathbb{Q}}$, the numbers $a_p = \psi(T_p)$ are algebraic integers. We would like to give them some geometric meaning. Let's take the example of $g_1(N) = 1$. Then $\overline{M_1(N)}$ is an elliptic curve E defined over $\mathbb{Z}[N^{-1}]$. Moreover we have an exact sequence of cohomology groups

$$0 \longrightarrow H^1(E(\mathbb{C}),\mathbb{Z}) \longrightarrow H^1(E(\mathbb{C}),\mathcal{O}_E) \longrightarrow H^1(E(\mathbb{C}),\mathcal{O}_E^\times) \longrightarrow H^2(E(\mathbb{C}),\mathbb{Z}).$$

As the image of the first map is a lattice, as the group $H^2(E(\mathbb{C}),\mathbb{Z})$ is torsion free and since $\mathrm{Pic}^0(E(\mathbb{C}))$ is divisible (isomorphic to $\overline{M_1(N)}(\mathbb{C})$), we obtain a short exact sequence

$$0 \longrightarrow H^1(E(\mathbb{C}),\mathbb{Z}) \longrightarrow H^1(E(\mathbb{C}),\mathcal{O}_E) \longrightarrow \mathrm{Pic}^0(E(\mathbb{C})) \longrightarrow 0.$$

Using the snake Lemma and the Abel-Jacobi isomorphism $E(\mathbb{C}) \simeq \mathrm{Pic}^0(E(\mathbb{C}))$, we obtain, for each prime number ℓ, an isomorphism

$$H^1(E(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell\mathbb{Z} \simeq E(\mathbb{C})[\ell] \simeq E(\overline{\mathbb{Q}})[\ell].$$

If p is a prime number non dividing $N\ell$, the group scheme $E[\ell]$ is finite étale over $\mathrm{Spec}\,\mathbb{Z}_p$, which gives us an isomorphism

$$E(\overline{\mathbb{Q}})[\ell] \simeq E(\overline{\mathbb{F}_p})[\ell].$$

The action of the Hecke T_p on $H^1(E(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}/\ell\mathbb{Z}$ comes, under this isomorphism, from an explicit isogeny of $E_{\mathbb{F}_p}$. This will give us a géométric interpretation of the algebraic integers modulo ℓ.

However, in the general case, the genus of $X_1(N)$ can be bigger than 1 and we have to replace the elliptic curve by an other group scheme attached to the curve $\overline{M_1(N)}$: its Jacobian variety.

7.3 Jacobian varieties of modular curves

The Picard functor We will only describe a very particular case. A more general situation is described in [BLR90, §8,9].

Let S be a scheme and X/S a proper and smooth curve. We assume that X is geometrically connected and that the map $f : X \to S$ has a section. Under these assumptions, we know that $\mathcal{O}_S \xrightarrow{\sim} f_*\mathcal{O}_X$ and that $f_*\mathcal{O}_X$ commutes to base change. The *Picard functor* of X/S is the contravariant functor associating to each S-schme T, the set

$$\mathrm{Pic}_{X/S}(T) \coloneqq \mathrm{Coker}(\mathrm{Pic}(T) \to \mathrm{Pic}(X \times_S T)).$$

As in the case of elliptic curves, given a section $\varepsilon : S \to X$ to f, we have a group homomorphism

$$\mathrm{Pic}_{X/S}(T) \simeq \{\mathcal{L} \in \mathrm{Pic}(X) \mid \varepsilon^*\mathcal{L} \simeq \mathcal{O}_S\}.$$

Similarly, we have a degree map $\deg : \mathrm{Pic}_{X/S} \to \mathbb{Z}$ and we define $\mathrm{Pic}^0_{X/S}$ as its kernel.

Theorem 7.3 (Weyl, Grothendieck)**.** *The functor* $\mathrm{Pic}^0_{X/S}$ *is representable by a projective and smooth* S*-scheme of relative dimension the genus of the relative curve* X/S*. Its fibres are geometrically connected.*

Remark 7.4. This theorem is still true without assuming the existence of the section $\varepsilon : S \to X$. However, in the general case, the definition of $\mathrm{Pic}_{X/S}$ is more involved.

This theorem implies that $\mathrm{Pic}^0_{X/S}$ is a projective S-group scheme called the *jacobian* of the curve X. We will note it $J(X/S)$. This is a particular case of abelian variety.

Abelian varieties An *abelian variety* over a scheme S is a projective and smooth S-group scheme with geometrically connected fibres. An elliptic curve is an abelian variety of relative dimension 1. Conversely, it can be proved that an abelian variety of dimension 1 is an elliptic curve, so that the notion of abelian variety is a generalisation of the notion of elliptic curve. If X/S is a projective and smooth curve with geometrically connected fibres, its jacobian is an abelian variety over S.

Example 7.5. There is a generalisation of the complex uniformisation theorem. An abelian variety over $\mathbb{C}$ is a complex torus. More precisely, if $A/\mathbb{C}$ is an abelian variety of dimension g. There exists a lattice $\Lambda \subset \mathbb{C}^g$ and an isomorphism of complex analytic groups

$$\mathbb{C}^g/\Lambda \simeq A(\mathbb{C})^{\mathrm{an}}.$$

However if $g \geqslant 2$, all lattices $\Lambda \subset \mathbb{C}^g$ don't come from abelian varieties ([Mum08, Part I]).

As for elliptic curves, we have the following result.

Theorem 7.6. *Let A/S be an abelian variety. Let $N \geqslant 1$. The multiplication by N map $[N] : A \to A$ is finite and locally free of degree N^{2g} and étale if moreover $N \in \Gamma(S, \mathcal{O}_S)^\times$.*

When S is a regular scheme with generic points of characteristic 0, it can be proved exactly as for elliptic curves.

An *isogeny* between abelian varieties is a morphism of group schemes which is finite and locally free.

Fonctorialities of jacabians Let $f : X \to Y$ be a morphism between projective and smooth curves with geometrically connected fibres. The functoriality of the Picard group gives a natural map

$$f^* : J(Y/S) \to J(X/S)$$

which is a morphism of abelian varieties. It sends an invertible sheaf $\mathcal{L}$ on $f^*\mathcal{L}$. We can give an other description of this map in terms of divisors. Assume that $S = \operatorname{Spec} k$ where k is an algebraically closed field. The description of invertible sheaves on X in terms of divisors gives us a group homomorphism

$$J(Y/S)(k) \simeq \mathrm{Div}^0(Y)/\operatorname{div}(k(Y)^\times).$$

Then we have

$$f^*\left(\sum_{Q \in Y(k)} n_Q(Q)\right) = \sum_{Q \in Y(k)} n_Q[f^{-1}(Q)] = \sum_{Q \in Y(k)} \sum_{P \in f^{-1}(Q)} n_Q e_P(f).$$

However we can also define a morphism $f_* : J(X/S) \to J(Y/S)$. This morphism is defined as follows. We can assume that S is connected. If f is constant, then f

is finite and locally free. As the fibres of X/S and Y/S are connected, X and Y are connected and the degree d of f is constant. Let $\mathcal{L}$ be some invertible sheaf over X. Let $\operatorname{Spec} A$ be some affine open subset in Y and let $\operatorname{Spec} B = f^{-1}(\operatorname{Spec} A)$. Then B is finite projective A-module of rank d and $\mathcal{L}|_{\operatorname{Spec} B}$ comes form a projective B-module M of rank 1. Consequently $\Lambda^d_A M$ is a projective A-module of rank 1. The A-modules $\Lambda^d_A M$ can be glued on Y to give rise to an invertible sheaf $\Lambda\mathcal{L}$ on Y. It can be checked that $\Lambda(\mathcal{L}\otimes\mathcal{L}') \simeq \Lambda\mathcal{L}\otimes\Lambda\mathcal{L}'$ and that $\deg(\Lambda\mathcal{L}) = \deg(\mathcal{L})$, this gives a group morphism $\operatorname{Pic}^0(X/S) \to \operatorname{Pic}^0(Y/S)$. We can do this construction on all sets of T-points, which gives a morphisme of abelian varieties

$$f_* : J(X/S) \longrightarrow J(Y/S).$$

The following functorialities are easily checked

$$(g\circ f)^* = f^*\circ g^*, \quad (g\circ f)_* = g_*\circ f_*,$$

Moreover, we have $f^*\circ f_* = [\deg f]$.

If $S = \operatorname{Spec} k$ with k an algebraically closed field. The description of f_* on divisors is, for f non constant,

$$f_*\left(\sum_{P\in X(k)} n_P(P)\right) = \sum_{P\in X(k)} n_P(f(P)).$$

Let k be a field. If G/k is a smooth group scheme of relative dimension g, the sheaf of differentials Ω^1_G is free of rank g. Namely by smoothness the sheaf $\Omega^1_{G/k}$ is locally free of rank g. The global freeness comes from the fact that Ω^1_G is G-equivariant so that $\Omega^1_G \simeq \mathcal{O}_G\otimes(\Omega_G\otimes k(e))$ (see [DG70, I.Prop 6.8.1] for details). In greater generality, if $\pi : G\to S$ is a group scheme with neutral section ε, then $\Omega^1_{G/S} \simeq \pi^*(e^*\Omega_{G/S})$.

Assume that $\pi_1 : X \to S$ is a smooth and projective curve with geometrically connected fibres. Then we can define morphism of S-schemes $f : X \to J(X/S)$ sending a section $s\in X(T)$ to the invertible sheaf of degree 0 : $\mathcal{L}(s)\otimes\mathcal{L}(\varepsilon)^{-1}$ on X. Writing $\pi_2 : J(X/S)\to S$ for the structural map, we obtain a morphism $\Omega^1_{J(X/S)/S} \to f_*\Omega^1_{X/S}$ and, by pushforward, a map

$$\pi_{2,*}\Omega^1_{J(X/S)} \longrightarrow \pi_{1,*}\Omega^1_{X/S}.$$

I claim that this map is an isomorphism of coherent sheaves. Namely, let $\omega_{X/S} \coloneqq e^*\Omega^1_{J(X/S)}$ (with e the neutral section), then $\Omega^1_{J(X/S)} \simeq \pi_2^*\omega_{X/S}$ and $\omega_{X/S} \simeq \pi_{2,*}\Omega^1_{J(X/S)}$. We have to check that the map $\omega_{X/S}\to\pi_{1,*}\Omega^1_{X/S}$ is an isomorphism. However, we know that $\operatorname{Lie}(J(X/S)/S) \simeq \mathbb{V}(\omega_{X/S})$. The description of the functor of points of $J(X/S)$ tells us that

$$\operatorname{Lie}(J(X/S)/S)(T) = \operatorname{Ker}(J(X/S)(T[\varepsilon]) \to J(X/S)(T)).$$

As the set of isomorphism classes of line bundles on a scheme Y is in natural bijection with $H^1(Y, \mathcal{O}_Y^\times)$, we deduce that $\mathrm{Lie}(J(X/S)/S) \simeq \mathbb{V}((R^1\pi_{1,*}\mathcal{O}_X)^\vee)$ and an isomorphism of coherent sheaves $(R^1\pi_{1,*})^\vee\mathcal{O}_X \simeq \omega_{X/S}$ (note that $R^1 f_*\mathcal{O}_X$ is locally free since X/S is proper and smooth). We obtain a map $(R^1 f_*\mathcal{O})^\vee \to \pi_{1,*}\Omega^1_{X/S}$. To prove that this map is an isomorphism can be checked fibrewise. We are reduced to the situation where $S = \mathrm{Spec}\, k$ for a field k and this is then a consequence of Serre duality.

If $S = \mathrm{Spec}\, k$, this implies that the map

$$H^0(J(X/k), \Omega^1_{J(X/k)}) \longrightarrow H^0(X, \Omega^1_{X/k})$$

is an isomorphism.

7.4 Applications to spaces of modular forms

We fix some integer N and we consider the curve $X = \overline{M_1(N)}$ which is projective and smooth over $\mathrm{Spec}\,\mathbb{Z}[N^{-1}]$ with geometrically connected fibres. Let $J_1(N)$ be the jacobian of $\overline{M_1(N)}$, which is an abelian variety over $\mathrm{Spec}\,\mathbb{Z}[N^{-1}]$. Note that, with our naive definition of the Picard functor, we need the existence of section on X. This can be realised by cusps. However we won't go in this details.

Assume that $N \geqslant 4$, so that $M_1(N)$ is the moduli space $\mathcal{M}(\Gamma_1(N))$. Let $\mathcal{E}$ be the universal elliptic curve over $\mathcal{M}(\Gamma_1(N))$. Let p be a prime number not dividing N and let $\mathcal{M}_1(N,p) \coloneqq [\Gamma_0(p)]_{\mathcal{E}/\mathcal{M}(\Gamma_1(N))}$. The map $\mathcal{M}_1(N;p) \to \mathcal{M}(\Gamma_1(N))$ is finite and étale if we inverse p. Moreover the scheme $\mathcal{M}_1(N;p) \to \mathcal{M}(\Gamma_1(N))$ represents the functor sending a $\mathbb{Z}[(Np)^{-1}]$-scheme S to the set of isomorphism classes of triple (E, P, H) where E is an elliptic curve over S, P is a section of order N of $E[N]$ and $H \subset E[p]$ is a finite étale subgroup-scheme of order p.

There are actually two maps $\mathcal{M}_1(N;p) \to \mathcal{M}(\Gamma_1(N))$. The first one, that we name π_1, is the map $(E, P, H) \mapsto (E, P)$ obtained by forgetting H. The second one, that we name π_2, is the map $(E, P, H) \mapsto (E/H, P)$ where E/H is the quotient of E by the subgroup H and P is the image of P by the group homomorphism $E[N](S) \to (E/H)[N](S)$. Note that the isogeny $E \to E/H$ has degree p, so that the previous homomorphism is injective since $p \nmid N$ and the image of P in $(E/H)[N](S)$ has order N. We have two morphisms of $\mathrm{Spec}\,\mathbb{Z}[(Np)^{-1}]$-schemes

$$\begin{array}{ccc} & \mathcal{M}_1(N;p) & \\ {\scriptstyle \pi_1}\swarrow & & \searrow{\scriptstyle \pi_2} \\ \mathcal{M}(\Gamma_1(N)) & & \mathcal{M}(\Gamma_1(N)). \end{array}$$

The complex points of $\mathcal{M}_1(N;p)$ are in bijection with $Y(\Gamma_1(N) \cap \alpha_p \Gamma_1(N) \alpha_p^{-1})$. So that

on complex points, we have to maps of Riemann surfaces

$$\begin{array}{ccc} & Y(\Gamma_1(N) \cap \alpha_p \Gamma_1(N) \alpha_p^{-1}) & \\ \swarrow^{\pi_1} & & \searrow^{\pi_2} \\ Y(\Gamma_1(N)) & & Y(\Gamma_1(N)) \end{array}$$

Now it is a simple computation to check that it coincides, after restriction to $Y(\Gamma_1(N))$ and $Y(\Gamma_1(N) \cap \alpha_p \Gamma_1(N) \alpha_p^{-1})$ with the maps of the diagram (11).

We define $T_p \coloneqq \pi_{2,*} \circ \pi_1^* \in \operatorname{End} J_1(N)_{\mathbb{Z}[(Np)^{-1}]}$. This is an endomorphism of the abelian variety $J_1(N)_{\mathbb{Z}[(Np)^{-1}]}$. It induces an endomorphism of the complex vector space

$$H^0(J_1(N)_{\mathbb{C}}, \Omega^1_{J_1(N)_{\mathbb{C}}}) \simeq H^0(Y_1(N), \Omega_{Y_1(N)}).$$

This endomorphism preserves $S_2(\Gamma_1(N))$ and coincides with the Hecke operator T_p.

If $d \wedge N = 1$, we can also define an endomorphism $\langle d \rangle$ of $J_1(N)$. It is the endomorphism $\langle d \rangle_*$ where $\langle d \rangle$ is the endomorphism of $\mathcal{M}_1(N)$ given by $(E, P) \mapsto (E, dP)$ on points and extended uniquely to $\overline{M_1(N)}$ by normalisation. The operators T_p and $\langle d \rangle$ commutes, this gives us an action of the algebra $\mathcal{H}_2^{(N)}(\Gamma_1(N))$ on the abelian variety $J_1(N)$.

8 Galois representations

8.1 Some generalities

Let K be a field and $\overline{K}$ some algebraic closure of K. We use the notation $\mathcal{G}_K$ for the topological group $\operatorname{Gal}(K^s/K)$ of the separable closure K^s of K in $\overline{K}$. It is a totally disconnected topological group.

Let ℓ be some prime number. A *ℓ-adic representation* of $\mathcal{G}_K$ is a pair (ρ, V) where V is a finite dimension $\mathbb{Q}_\ell$-vector space and ρ is a continuous group homomorphism $\mathcal{G}_K \to \mathrm{GL}_{\mathbb{Q}_\ell}(V)$. A morphism of ℓ-adic representations $(\rho_1, V_1) \to (\rho_2, V_2)$ is a $\mathbb{Q}_\ell$-linear map $f : V_1 \to V_2$ such that

$$\forall g \in \mathcal{G}_K, \quad \rho_2(g) \circ f = f \circ \rho_1(g).$$

If E is a finite extension of $\mathbb{Q}_\ell$ and (ρ, V) is an ℓ-adic representation of $\mathcal{G}_K$, we say that (ρ, V) is an E-representation if V has an additional structure of E-vector space and if $\rho(\mathcal{G}_K) \subset \mathrm{GL}_E(V)$.

Remark 8.1. There is an obvious bijection between the set of isomorphism classes of E-representations of $\mathcal{G}_K$ and the set of conjugation classes of continuous homomorphisms $\mathcal{G}_K \to \mathrm{GL}_n(E)$.

The *dimension* of an E-representation of $\mathcal{G}_K$ is the dimension of V as an E-vector space.

Let (ρ, V) be some E-representation of $\mathcal{G}_K$. Then there exists some $\mathcal{O}_E$-lattice V° (a finite free $\mathcal{O}_E$-module such that $V^\circ[\frac{1}{\ell}] = V$) in V which is stable under the action of the group $\mathcal{G}_K$. Namely let V° be *some* $\mathcal{O}_E$-lattice in V. Then V° is an open subset of V. This implies that the subgroup

$$H \coloneqq \{g \in \mathcal{G}_K \mid \rho(g)V^\circ \subset V^\circ\}$$

is contained open in $\mathcal{G}_K$. As $\mathcal{G}_K$ is compact, the subgroup H is of finite index in $\mathcal{G}_K$. We can find elements $g_1, \ldots, g_r$ such that

$$\mathcal{G}_K = \coprod_{i=1}^{r} H g_i$$

and the set $\sum_{i=1}^r \rho(g_i)V^\circ$ is a lattice in V which is stable under the group $\mathcal{G}_K$.

So we can fix an $\mathcal{O}_E$-lattice $V^\circ \subset V$ which is stable under the action of $\mathcal{G}_K$. If $n \geqslant 1$ is an integer, the sub-lattice $\ell^n V^\circ$ is also stable under $\mathcal{G}_K$ and the group $\mathcal{G}_K$ acts continuously on the *finite* group $V^\circ/\ell^n V^\circ$. This implies that the morphism

$$\mathcal{G}_K \xrightarrow{\rho} \mathrm{GL}_{\mathcal{O}_E}(V^\circ) \to \mathrm{GL}_{\mathcal{O}_E}(V^\circ/\ell^n V^\circ)$$

factors through a finite quotient of $\mathcal{G}_K$.

First of all, we will give some example of ℓ-adic representations of Galois groups.

Example 8.2. 1) Assume that ℓ is different from the characteristic of K. The group $\mathcal{G}_K$ acts on $\overline{K}$ and preserves the subgroups $\mu_{\ell^n}(\overline{K})$ of ℓ^n-th roots of 1. If we fix a primitive ℓ^n-th root of 1, we obtain a group homomorphism $\mu_{\ell^n}(\overline{K}) \simeq \mathbb{Z}/\ell^n\mathbb{Z}$. Moreover the extension $K(\mu_{\ell^n}(\overline{K}))/K$ is finite so that the action of $\mathcal{G}_K$ on $\mu_{\ell^n}(\overline{K})$ factors through a finite quotient of $\mathcal{G}_K$. The raising to the ℓ-th power gives us a map $\mu_{\ell^{n+1}}(\overline{K}) \to \mu_{\ell^n}(\overline{K})$ which is surjective and commutes to the action of $\mathcal{G}_K$. Consequently the group $\mathcal{G}_K$ acts on the projective limit

$$T_\ell(\mu) \coloneqq \varprojlim_{n \geqslant 1} \mu_{\ell^n}(\overline{K}).$$

It is a $\mathbb{Z}_\ell$-module which can be check to be free of rank 1 (a compatible system of primitive ℓ^n-th roots of unity provides a basis). Moreover the surjection $T_\ell(\mu) \twoheadrightarrow \mu_{\ell^n}(\overline{K})$ induces an isomorphism

$$T_\ell(\mu)/\ell^n T_\ell(\mu) \simeq \mu_{\ell^n}(\overline{K})$$

of finite modules on which $\mathcal{G}_K$ acts through a finite quotient. This proves that the action of $\mathcal{G}_K$ on $T_\ell(\mu)$ is continuous. We define $V_\ell(\mu) \coloneqq T_\ell(\mu) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. This is an ℓ-adic representation of $\mathcal{G}_K$ of dimension 1. There is a canonical isomorphism $\mathbb{Q}_\ell^\times \simeq \mathrm{GL}_{\mathbb{Q}_\ell}(V_\ell(\mu))$ so that this representation is given by a continuous character $\chi_\ell : \mathcal{G}_K \to \mathbb{Q}_\ell^\times$. This character is called the *cyclotomic character*, its image is actually contained in the maximal compact subgroup $\mathbb{Z}_\ell^\times \subset \mathbb{Q}_\ell^\times$.

2) Let χ be a Dirichlet character. This is character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Actually, since the image of χ is a finite subgroup of $\mathbb{C}^\times$, it is contained in some number field $E \subset \mathbb{C}$. We can associate to χ a group homomorphism

$$\mathcal{G}_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} E^\times.$$

Now if λ is a finite place of E, we can compose this character with $E^\times \subset E_\lambda^\times$ to obtain a 1-dimension E_λ-representation of $\mathcal{G}_\mathbb{Q}$.

3) Let E be an elliptic curve defined over the field K. If ℓ is different from the characteristic of K, we defined the *Tate module*

$$T_\ell E \coloneqq \varprojlim_{n \geqslant 1} E[\ell^n](\overline{K})$$

and we proved that $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is 2-dimensional $\mathbb{Q}_\ell$-vector space and the group $\mathcal{G}_K$ acts $\mathbb{Q}_\ell$-linearly and continuously on $V_\ell(E)$.

4) More generally if A is an abelian variety defined over K and ℓ is different from the characteristic of K, we can define the ℓ-adic *Tate module* of A as being

$$T_\ell(A) \coloneqq \varprojlim_{n \geqslant 1} A[\ell^n](\overline{K})$$

and $V_\ell(A) =\coloneqq T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is an ℓ-adic representation of $\mathcal{G}_K$ of dimension $2\dim(A)$. When K is a number field, the ℓ-adic representation $V_\ell(A)$ encodes lots of geometric and arithmetic informations about A. This topic is related to *Tate conjecture* which is still widely open.

Now we will focus on the case where K is a number field. Let Σ_K be the set of finite places of K. Let $v \in \Sigma_K$, it corresponds to a non zero prime ideal $\mathfrak{p}_v \subset \mathcal{O}_K$. The residue field $k_v \coloneqq \mathcal{O}_K/\mathfrak{p}_v$ is finite and let $Nv = p_v^{\deg(v)}$ be its cardinal (here p_v is the unique prime number such that $\mathfrak{p}_v \cap \mathbb{Z} = (p_v)$). Let w be a place of $\overline{Q}$ above v and let $D_w \subset \mathcal{G}_K$ be the decomposition group at w and $I_w \subset D_w$ its inertia subgroup. We have then a group isomorphism $D_w/I_w \simeq \mathrm{Gal}(\overline{k_v}/k_v)$. Let $\mathrm{Frob}_w \in \mathrm{Gal}(\overline{k_v}/k_v)$ be the element inducing $x \mapsto x^{Nv}$ on $\overline{k_v}$, it is actually a generator of this group (which is cyclic of order Nv). We say that an ℓ-adic representation (ρ, V) of $\mathcal{G}_K$ is *unramified at* w if $\rho(I_w) = \{1\}$. In this case the element $\rho(\mathrm{Frob}_w)$ is well defined (it does not depend of a lifting of Frob_w in D_w). Note that for two places w and w' above v, the subgroups D_w and $D_{w'}$ are conjugated in $\mathcal{G}_K$. Moreover, if h is such that $hD_wh^{-1} = D_{w'}$, and $\widetilde{\mathrm{Frob}}_w$ is a lifting of Frob_w, then $h\widetilde{\mathrm{Frob}}_w h^{-1}$ is a lifting of $\mathrm{Frob}_{w'}$. This proves that, if (ρ, V) is unramified at a place w above v, it is unramified at all places w above v and that the conjugacy class of $\rho(\mathrm{Frob}_w)$ does not depend on the choice of w. We use the notation $F_{v,\ell}$ for this conjugacy class.

Example 8.3. 1) Assume that χ is a Dirichlet character. The *conductor* of χ is the smallest integer N such that χ comes from a character of $(\mathbb{Z}/N\mathbb{Z})^\times$. The finite places of

$\mathbb{Q}$ correspond to the prime numbers and the ℓ-adic Galois representation associated to χ is unramified exactly at the prime numbers which does not divide $N\ell$. If p is such a prime, then $F_{p,\chi} = \chi(p) \in \mathbb{Z}_\ell^\times$.

2) Let χ_ℓ be the ℓ-adic cyclotomic character. Then χ_ℓ is unramified at all prime numbers different from ℓ and $F_{p,\chi_\ell} = p \in \mathbb{Z}_\ell^\times$.

3) Let $(\rho, V_\ell(E))$ be the ℓ-adic representation associated to an elliptic curve E defined over $\mathbb{Q}$. Then $(\rho, V_\ell(E))$ is unramified exactly at the prime numbers p which are different from ℓ and such that E has good reduction at p. Namely, in this case, the torsion group $E[\ell^n]$ is a finite étale group scheme over $\operatorname{Spec}\mathbb{Z}_p$, so that the action of the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on $E[\ell^n]$ is trivial. If p is such a prime, then $F_{p,\ell}$ is a conjugation class in $\mathrm{GL}_2(\mathbb{Q}_\ell)$ whose characteristic polynomial is $X^2 - a_p X + p$ where a_p is the Hasse defect $p + 1 - |E(\mathbb{F}_p)|$.

We will slightly generalise this situation. Let F be a finite extension of $\mathbb{Q}_\ell$ and let $E \subset F$ be a subfield which is also a number field. A F-representation (ρ, V) is said *E-rational* if there exists a finite subset $S \subset \Sigma_K$ such that ρ is unramified outside of S and if, for all $v \in \Sigma_K \smallsetminus S$, the conjugacy class $F_{\rho,v}$ has a characteristic polynomial which is in $E[X]$.

Now let E be some number field and λ, λ' two places of E and $E_\lambda, E_{\lambda'}$ be the completions of E at λ and λ'. Let (ρ, V) (resp. (ρ', V')) be some E_λ-representation (resp. $E_{\lambda'}$-representation) of $\mathcal{G}_K$. These two representations are said to be *compatible* (even if they are defined on vector spaces corresponding to different scalar fields) if they are both E-rational and if there exists a finite subset $S \subset \Sigma_K$ such that, for all $v \in \Sigma_K \smallsetminus S$ the two representations ρ and ρ' are unramified at v and the characteristic polynomials of $F_{\rho,v}$ and $F_{\rho',v}$ coincide in $E[X]$.

Remark 8.4. Using Chebotarev density theorem, we can prove that if (ρ, V) is some E-rational E_λ-representation, and if λ' is a finite place of E, there is at most one semisimple $E_{\lambda'}$-representation of $\mathcal{G}_K$ which is compatible with (ρ, V).

Let $(\rho_\lambda, V_\lambda)$ be a family of E_λ-representations of $\mathcal{G}_K$ indexed by the finite places of E. Such a family is said to be *compatible* if the representations are pairwise compatible. Such a family if said to be *strictly compatible* if there exists a finite subset $S \subset \Sigma_K$ such that for all pair of places (λ, λ') of E and for all place $v \notin S$ and not above the same prime number that λ and λ', the representations ρ_λ and $\rho_{\lambda'}$ are unramified at v and the characteristic polynomials of $F_{\rho_\lambda,v}$ and $F_{\rho_{\lambda'},v}$ coincide.

Example 8.5. If E is an elliptic curve defined over $\mathbb{Q}$, the system of Galois representations $(V_\ell(E))$, where ℓ is varying among the prime numbers, is a strictly compatible system of Galois representations. Actually all the examples given previously are compatible systems of Galois representations.

If $(\rho_\lambda, V_\lambda)$ is a strictly compatible system of Galois representations, we can define a (partial) L-function. Namely fix a finite subset $S \subset \Sigma_K$ as in the definition. If $v \notin S$,

we can find some place λ such that v and λ are not over the same prime number and consider the characteristic polynomial $P_v(X)$ which *does not depend on* λ by definition. The partial L-function of the system is (without considering any convergence issues)

$$L(s) = \prod_{v \notin S} \frac{1}{\det(1 - \rho_\lambda(\mathrm{Frob}_v) N v^{-s})}.$$

In the case of the system associated to Dirichlet character, we recover the Dirichlet L-function of the character, in the case of an elliptic curve, we recover the L-function of the elliptic curve etc. It is therefore natural, since we can construct an L-function with Eulerian product associated to a proper modular form, if it is possible to associate a strictly compatible system of Galois representations to a proper modular form.

According to the following theorem, the answer is yes.

Theorem 8.6 (Eichler, Shimura, Kuga, Deligne)**.** *Let $k \geqslant 2$, $N \geqslant 1$ and let $f \in S_k(\Gamma_1(N))$ be a normalised modular eigenform. Let*

$$\tilde{f}(q) = q + \sum_{n \geqslant 2} a_n q^n$$

be its Fourier series. Let K_f be the number field generated by the coefficients of f and let λ be a finite place of K_f over some prime number ℓ of $\mathbb{Q}$. Then there exists a Galois representation $(\rho_{f,\lambda}, V_{f,\lambda})$ of $\mathcal{G}_\mathbb{Q}$ such that

(i) the representation $\rho_{f,\lambda}$ is unramified at all prime numbers p which does not divide $N\ell$;

(ii) if p is a prime number which does not divide $N\ell$, then the characteristic polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ is $X^2 - a_p X + \chi(p)p^{k-1}$ where χ is the character of $(\mathbb{Z}/N\mathbb{Z})^\times$ such that $\langle d \rangle f = \chi(d) f$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Then the system $(\rho_{f,\lambda}, V_{f,\lambda})$ is a strictily compatible system of 2-dimensional Galois representations.

We will give a proof of this theorem in the case where $k = 2$. In this case (due to Eichler and Shimura), the construction of the Galois representation can be done using the Jacobian variety attached to a modular curve. The general case (due to Deligne) is more complicated, we have then to replace the Jacobian variety by the étale cohomology (with coefficients) of the modular curves.

8.2 Construction of the Galois representation in weight 2

Let $f \in S_2(\Gamma_1(N), \chi)^{\mathrm{new}}$ be a new eigenform. Let $J_1(N)_{/\mathbb{Q}}$ be the jacobian variety of the proper and smooth modular curve $X_1(N)$. It is an abelian variety defined over $\mathbb{Q}$ of dimension $g_1(N)$.

If ℓ is a prime number, we can consider the ℓ-adic Galois representation

$$V_\ell J_1(N) \coloneqq T_\ell J_1(N) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell, \qquad T_\ell J_1(N) \coloneqq \varprojlim_n J_1(N)[\ell^n](\overline{\mathbb{Q}}) \simeq \mathbb{Z}_\ell^{2g}$$

where $g = g_1(N)$. There is a continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_\ell J_1(N)$ and $T_\ell J_1(N)/\ell^n \simeq J_1(N)[\ell^n](\overline{\mathbb{Q}})$ for all $n \geqslant 1$.

Let $\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}$ be the image of the algebra $\mathcal{H}^{(N)}(\Gamma_1(N))$ in $\mathrm{End}\, S_2(\Gamma_1(N))$. As seen previously, there is a natural action of $\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}$ on $J_1(N)_\mathbb{Q}$ which is compatible with the isomorphism $S_2(\Gamma_1(N)) \simeq H^0(X_1(N)_\mathbb{C}, \Omega^1) \simeq H^0(J_1(N)_\mathbb{Q}, \Omega^1) \otimes_\mathbb{Q} \mathbb{C}$.

The new eigenform f gives rise to character $\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z} \to K_f$ whose image is an order $\mathcal{O}_f$ inside K_f. Let $\mathfrak{p}_f$ be the kernel of this map, this is a prime ideal of $\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z} \to K_f$. We define, for a prime number ℓ,

$$T_\ell(f) \coloneqq T_\ell J_1(N) \otimes_{\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}} \mathcal{O}_f, \qquad V_\ell(f) \coloneqq T_\ell(f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Proposition 8.7. *The $\mathbb{Z}_\ell \otimes_\mathbb{Z} \mathcal{O}_f$-module $T_\ell(f)$ is finite free of rank 2. Consequently the $\mathbb{Q}_\ell \otimes_\mathbb{Q} K_f$-module $V_\ell(f)$ is finite free of rank 2.*

Proof. For $n \geqslant 1$, we have isomorphisms of $\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}$-modules

$$T_\ell(f)/\ell^b \simeq J_1(N)[\ell^n](\overline{\mathbb{Q}}) \simeq J_1(N)[\ell^n](\mathbb{C})$$

the second isomorphism coming from the fact that $J_1(N)[\ell^n]$ is a finite $\overline{\mathbb{Q}}$-scheme. Moreover, it follows from the uniformisation of abelian varieties over $\mathbb{C}$ that

$$J_1(N)[\ell^n](\mathbb{C}) = J_1(N)(\mathbb{C})[\ell^n] \simeq H_1(J_1(N)(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}/\ell^n\mathbb{Z}.$$

This isomorphism is compatible to the action of $\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}$. Namely this ring is acting by endomorphisms of $\mathbb{Q}$-schemes on $J_1(N)$. Therefore, we are done if we can prove that $H_1(J_1(N)(\mathbb{C}), \mathbb{Z}) \otimes_{\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}} \mathcal{O}_f$ is isomorphic to $\mathcal{O}_f^2$ up to torsion, ie if $H_1(J_1(N)(\mathbb{C}), \mathbb{Z}) \otimes_{\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}} K_f$ is a two dimensional K_f-vector space. Let $\tau : K_f \hookrightarrow \mathbb{C}$ and let λ_τ be the composite

$$\mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z} \xrightarrow{\lambda_f} K_f \xrightarrow{\tau} \mathbb{C}.$$

it is sufficient to prove that $H_1(J_1(N)(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z},\tau} \mathbb{C}$ is a 2-dimensional vector space. By duality, it is sufficient to prove that the sub-$\mathbb{C}$-vector space of $H^1(J_1(N)(\mathbb{C}), \mathbb{C})$ of vectors v such that

$$\forall T \in \mathcal{H}_2^{(N)}(\Gamma_1(N))_\mathbb{Z}, \quad Tv = \lambda_\tau(T)v$$

is 2-dimensional.

Let's recall that we constructed by integration a $\mathbb{C}$-linear injective map

$$S_2(\Gamma_1(N)) \hookrightarrow \mathrm{Hom}(H_1(X_1(N), \mathbb{Z}), \mathbb{C}) \simeq H^1(X_1(N), \mathbb{Z}) \otimes \mathbb{C}$$

which is moreover a map of $\mathcal{H}_2^{(N)}(\Gamma_1(N))$-modules. Let $\overline{S_2(\Gamma_1(N))}$ be the image of $S_2(\Gamma_1(N))$ under the $\mathbb{R}$-linear automorphism of $H^1(X_1(N),\mathbb{Z})\otimes\mathbb{C}$ inducing the identity on $H^1(X_1(N),\mathbb{Z})$ and the complex conjugation on $\mathbb{C}$. As $H_1(X_1(N),\mathbb{Z})$ is generated by some $\mathbb{R}$-basis of $\mathrm{Hom}_{\mathbb{C}}(S_2(\Gamma_1(N)),\mathbb{C})$, we can check that we have

$$H^1(X_1(N),\mathbb{C}) = S_2(\Gamma_1(N)) \oplus \overline{S_2(\Gamma_1(N))}.$$

Note that this decomposition can also be seen as a consequence of the Hodge decomposition. Let $\overline{\tau}$ be the complex conjugate of τ. It follows from the discussion following Corollary 3.40 that $S_2(\Gamma_1(N))[\lambda_\tau]$ is one-dimensional. Consequently

$$H^1(X_1(N),\mathbb{C})[\lambda_\tau] \simeq S_2(\Gamma_1(N))[\lambda_\tau] \oplus S_2(\Gamma_1(N))[\lambda_{\overline{\tau}}]$$

is 2-dimensional over $\mathbb{C}$. □

Let $\lambda : K_f \hookrightarrow \overline{\mathbb{Q}_\ell}$ be an embedding of K_f in an algebraic closure $\overline{\mathbb{Q}_\ell}$ of $\mathbb{Q}_\ell$ and let $K_{f,\lambda}$ be the closure of $\lambda(K_f)$ in $\overline{\mathbb{Q}_\ell}$. This is a finite extension of $\mathbb{Q}_\ell$. We define

$$V_\lambda(f) \coloneqq V_\ell(f) \otimes_{\mathbb{Q}_\ell} K_{f,\lambda}.$$

This is a 2-dimensional $K_{f,\lambda}$-representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Theorem 8.8. *The $K_{f,\lambda}$-representation $V_\lambda(f)$ is unramified outside of $N\ell$.*

Proof. The scheme $J_1(N)$, the jacobian variety of the proper and smooth $\mathbb{Z}[N^{-1}]$-scheme $\overline{M_1(N)}$ is an abelian scheme over $\mathrm{Spec}\,\mathbb{Z}[N^{-1}]$. Consequently the group scheme $J_1(N)[\ell^n]$ is finite étale of rank $2g$ (with $g = g_1(N)$) over $\mathrm{Spec}\,\mathbb{Z}[(N\ell)^{-1}]$. This implies that the action of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \pi_1(\mathrm{Spec}\,\mathbb{Q}, \mathrm{Spec}\,\overline{\mathbb{Q}})$ factors through $\pi_1(\mathrm{Spec}\,\mathbb{Z}[(N\ell)^{-1}], \mathrm{Spec}\,\overline{\mathbb{Q}})$ which coincides with $\mathrm{Gal}(L/\mathbb{Q})$ where $L \subset \overline{\mathbb{Q}}$ is the largest sub-extension unramified outside of $N\ell$. This implies the claim. □

8.3 Eichler-Shimura congruences

Theorem 8.8 implies half of theorem 8.6 when $k = 2$. It remains to prove that, for a prime p not dividing $N\ell$, we have

$$\mathrm{Tr}(\mathrm{Frob}_p \mid V_\lambda(f)) = a_p(f), \qquad \det(\mathrm{Frob}_p \mid V_\lambda(f)) = p\chi(p).$$

In order to prove theses relations, we will use the fact that $J_1(N)$ has a good reduction at the prime p, ie that $J_1(N) \times_{\mathrm{Spec}\,\mathbb{Z}} \mathrm{Spec}\,\mathbb{F}_p$ is a proper and smooth $\mathbb{F}_p$-scheme. Then, for $p \nmid N$, the automorphism T_p of $J_1(N)_{\mathbb{Q}}$ can be extended to an automorphism over $\mathrm{Spec}\,\mathbb{Z}[(Np)^{-1}]$. We want to extend it into an automorphism of $J_1(N)$ over $\mathrm{Spec}\,\mathbb{Z}[N^{-1}]$. One of the difficulty is that we didn't give a definition of a structure of level p in characteristic p (the p-torsion group of an elliptic curve in characteristic p is not étale). This is possible but beyond the framework developed here. We will thus use the following trick :

Proposition 8.9. *Let R be a complete discrete valuation ring and let A be an abelian variety over R. Let $K = \operatorname{Frac} R$ be the fraction field of R and k the residue field of R. If $T \in \operatorname{End} A_K$ is an automorphism of the generic fiber A_K of A, then T extends uniquely into an endomorphism of A.*

Proof. The uniqueness is a direct consequence of the density of A_K in A. By étale descent, we are reduced to the case where k is separably closed. By unicity, we can consider U the largest open subset of A on which is defined a morphism $U \to A$ extending T. As A is projective and smooth, by the valuative criterion of properness, the set U contains all points of codimension 1, hence the generic point of the special fiber A_k, so that we have $U \cap A_k \neq \emptyset$. We have $A_K \subset U$, so that it is sufficient to prove that $A_k \subset U$. Let $V = A_k \cap U$ which is a non zero open subset of A_k. As A_k is of finite type over $\operatorname{Spec} k$, in order to show that $A_k = V$, it is sufficient to show that V contains all the closed points of A_k. Let $x \in A(k)$ be such a point. As A_k is irreducible, we have $V \cap (V - x) \neq \emptyset$. This implies that we can write $x = y - z$ with y and z inside $V(k)$. By smoothness of U over $\operatorname{Spec} R$, we can find $\tilde{y} \in U(R)$ lifting y and $\tilde{z} \in U(R)$ lifting z so that $\tilde{x} \coloneqq \tilde{y} - \tilde{z} \in A(R)$ is a point lifting x. We can define a morphism $T' : U + \tilde{x} \to A$ as the composition of the translation by $-\tilde{x}$, T and translation by $T(\tilde{y}) - T(\tilde{z})$. As T is a group homomorphism on A_K, we know that T and T' coincide in restriction to $U \cap A_K = (U + \tilde{x}) \cap A_K = A_K$. By density of A_K in A, they have to coincide on $U \cap (\tilde{x} + U)$ and we can extend T to $U \cap (\tilde{x} + U)$. By maximality of U, we have $\tilde{x} \in U(R)$. This implies that $x \in U(k)$. Finally we have proved that $U = A$. □

We deduce from this result that, for $p \nmid N$, the endomorphism T_p of $J_1(N)_{\mathbb{Q}_p}$ extends uniquely into an endomorphism of $J_1(N)_{\mathbb{Z}_p}$. After restriction to the fiber over $\mathbb{F}_p$, we obtain an endomorphism T_p of the abelian variety $J_1(N)_{\mathbb{F}_p}$.

8.4 Frobenius actions

In order to abbreviate notation, we will use $J_{\mathbb{F}_p} \coloneqq J_1(N)_{\mathbb{F}_p}$ and $k = \overline{\mathbb{F}_p}$. Let $F_{X_1(N)/\mathbb{F}_p} : X_1(N)_{\mathbb{F}_p} \to X_1(N)_{\mathbb{F}_p}$ be the absolute (or relative) Frobenius. We define, using covariance and contravariance properties of jacobians, two morphisms

$$F \coloneqq F_{X_1(N)/\mathbb{F}_p,*} : J_{\mathbb{F}_p} \to J_{\mathbb{F}_p}, \qquad V \coloneqq F^*_{X_1(N)/\mathbb{F}_p} : J_{\mathbb{F}_p} \to J_{\mathbb{F}_p}.$$

As $F_{X_1(N)/\mathbb{F}_p}$ is finite locally free of degree p, we deduce that F and V are two isogenies of $J_{\mathbb{F}_p}$ such that $V \circ F = F \circ V = [p]_{J_{\mathbb{F}_p}}$. Consequently F and V are endomorphisms of the abelian variety $J_{\mathbb{F}_p}$ of degree p^g. Let's describe them on some k-points of $J_{\mathbb{F}_p}$.

Let (E, P) be an k-point of $M_1(N)$, ie E is an elliptic curve over k and $P \in E[N](k)$ is a point of order N. Then the image of (E, P) by $F_{M_1(N))/\mathbb{F}_p}$ is the point $(E^{(p)}, P^{(p)})$ where $E^{(p)}$ is the inverse image of E by the Frobenius endomorphism of $\operatorname{Spec} k$ and $P^{(p)}$ is the image of P by the relative Frobenius $F_{E/k} : E \to E^{(p)}$. If $D = \sum_Q n_Q(Q)$ is an

effective divisor on $M_1(N)_{\mathbb{F}_p}$ (which can be seen as an effective divisor on $\overline{M_1(N)}_{\mathbb{F}_p}$ with support in $M_1(N)_{\mathbb{F}_p}$), then

$$F(D) = \sum_Q n_Q(F_{M_1(N)/\mathbb{F}_p}(Q))$$

where $F_{M_1(N)/\mathbb{F}_p}$ is described above. We also have

$$V(D) = \sum_Q \sum_{R \in F^{-1}_{M_1(N)/\mathbb{F}_p}(Q)} p n_Q(R)$$

since the ramification index of $F_{M_1(N)/\mathbb{F}_p}$ is p at all points of $M_1(N)_{\mathbb{F}_p}$.

Ordinary elliptic curves If k is an algebraically closed field of characteristic p, an elliptic curve E defined over k is *ordinary* if the following equivalent conditions are satisfied

- $E[p](k) \simeq \mathbb{Z}/p\mathbb{Z}$;
- $\forall n \geqslant 1$, $E[p^n](k) \simeq \mathbb{Z}/p^n\mathbb{Z}$;
- $\operatorname{Ker} V_E \simeq \mathbb{Z}/p\mathbb{Z}$;
- the map V_E is étale.

In a curve E is not ordinary, we say that it is *supersingular*.

Proposition 8.10. *Let E be a supersingular elliptic curve. Then its j-invariant $j(E)$ is contained $\mathbb{F}_{p^2} \subset k$. This implies that there is only a finite number of isomorphism classes of supersingular elliptic curves.*

Proof. If E is supersingular, the finite flat group $E[p]$ has no k-points, it is consequently a connected k-scheme. This implies that the inclusion $E[p] \subset E$ factors through $E[p] \hookrightarrow \operatorname{Spec} \mathcal{O}_{E,0}$ where $\mathcal{O}_{E,0}$ is the local ring of E at 0. In other words, as a scheme, $E[p]$ is isomorphic to $\operatorname{Spec} \mathcal{O}_{E,0}/I^n$ where I is the maximal ideal of $\mathcal{O}_{E,0}$. As $E[p]$ is a degree p^2 over $\operatorname{Spec} k$, we have $n = p^2$. This implies that $E[p]$ has a unique subgroups scheme of order p, which is $\operatorname{Spec} \mathcal{O}_{E,0}/I^p$. As a consequence, the subgroup schemes $\operatorname{Ker}(F^{(p)} : E^{(p)} \to E^{(p^2)})$ and $\operatorname{Ker}(V : E^{(p)} \to E)$ being both subgroup schemes of order p in $E^{(p)}[p]$ are actually equal. This implies that the map $V : E^{(p)} \to E$ factors through $F^{(p)}$ and induces (for degree reasons) an isomorphism between E and $E^{(p^2)}$:

$$\begin{array}{ccc} E^{(p)} & \xrightarrow{F^{(p)}} & E^{(p^2)} \\ & \searrow^{V} & \downarrow \wr \\ & & E \end{array}$$

As a consequence $j(E^{(p^2)}) = J(E)^{p^2} = J(E)$ and $j(E) \in \mathbb{F}_{p^2}$. □

Remark 8.11. We can prove that for each prime number p, there exists at least one supersingular curve in characteristic p (which is then defined over $\mathbb{F}_{p^2}$).

Corollary 8.12. *For $N \geqslant 4$, the set of points of $\overline{M_1(N)}(k)$ which are of the form (E, Q) with E supersingular is finite.*

Proof. Namely $\overline{M_1(N)}(k) \backslash M_1(N)(k)$ is finite and the set of points of the form (E, Q) is in contained in $j^{-1}(\mathbb{F}_{p^2})$ which is finite. □

Let R be a discrete valuation ring of residual characteristic p and generic characteristic 0. Let K be the fraction field of R. Let G be a finite flat group scheme over $\operatorname{Spec} R$ which is killed by p.

Lemma 8.13. *The map $H \mapsto H_K$ induces a bijection from the set of finite flat subgroups of G to the set of finite flat subgroups of G_K.*

Proof. We can define a map in the other direction. If $M \subset G_K$ is a finite flat subgroup. We can define $\overline{M}$ the schematic closure of M in G. As R is a principal ring, the R-scheme $\overline{M}$ is flat. Moreover $\overline{M}_K \simeq M$ since $M \subset G_K$ is closed. Conversely if $H \subset G$ is finite and flat over $\operatorname{Spec} R$, we have $\overline{H_K} \subset H$. For degree reasons, this inclusion is an equality. □

Now we assume moreover that the residue field k of R is algebraically closed. Let $E_{/R}$ be an elliptic curve over R such that the special fiber E_k is ordinary. Then the torsion group scheme $E[p]$ is finite flat over R and $E[p](k) \simeq \mathbb{Z}/p\mathbb{Z}$. This implies that the group of connected components $\pi_0(E[p])$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Consequently there exists a surjective morphism of group schemes

$$E \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})_R.$$

By Cartier duality, we deduce an injection of group schemes $(\mu_p)_R \hookrightarrow E[p]$. As μ_p is a connected group scheme (since $R[X]/(X^p - 1)$ is a local ring), we have $(\mu_p)_R \subset E[p]^\circ$. Comparing the degrees of these two group schemes, it is an equality. Now up to replace R by R' where R' is the integral closure of R in a finite extension K' of K, we can assume that $E[p](R') \simeq \mathbb{Z}/p\mathbb{Z}$, this gives us a section to the map $E \to (\mathbb{Z}/p\mathbb{Z})_R$ and induces an isomorphism of group schemes over R' :

$$E[p]_{R'} \simeq (\mu_p)_{R'} \times (\mathbb{Z}/p\mathbb{Z})_{R'}.$$

Now we can prove the main theorem, often known as "Eichler-Shimura" congruence.

Theorem 8.14. *In $\operatorname{End} J_{\mathbb{F}_p}$, we have an equality*

$$T_p = F + \langle p \rangle V.$$

Proof. Assume that $N \geqslant 4$, so that we have a moduli interpretation of the scheme $M_1(N) = \mathcal{M}(\Gamma_1(N))$.

As $J_{\mathbb{F}_p}$ is a geometrically reduced scheme of finite type over $\mathbb{F}_p$, it is sufficient to prove this equality for the corresponding endomorphisms of the group of k-points of $J_{\mathbb{F}_p}$. Let $Q \in \overline{M_1(N)}(k)$ be a point, then we have a morphism $\overline{M_1(N)}_k \to J_k$ which, on k-points is given by $P \mapsto (P)-(Q)$. Using the group scheme structure on $J_{\mathbb{F}_p}$, we deduce a morphism $\overline{M_1(N)}_k^g \to J_k$ which is given, on k-points, by $(P_1, \ldots, P_g) \mapsto \sum_{i=1}^g ((P_i) - (Q))$. Using Riemann-Roch theorem, we an check that this map is surjective on k-points.

Let $U \subset \overline{M_1(N)}_{\overline{\mathbb{F}_p}}$ be the open and dense subset corresponding to ordinary points. Assume moreover that the point Q (fixed a bit earlier) is ordinary. Then the map $U^g \to J_k$ is morphism of k-scheme with dense image. Therefore, in order to prove Eichler-Shimura relation, it is sufficient to prove that

$$T_p((x) - (x')) = (F + \langle p \rangle V)((x) - (x'))$$

for k-points x and x' in U. The points x and x' correspond to pairs (E, Q) and (E', Q') where E and E' are ordinary elliptic curves defined over $\overline{\mathbb{F}_p}$ and Q, Q' are points of E and E' of order N. However, we have a moduli description of the operator T_p only on points in characteristic prime to p, for example in characteristic 0. We will therefore "lift" the points x and x'.

As the scheme $M_1(N)$ is smooth over $\mathbb{Z}[N^{-1}]$, the points x and x' can be lifted into points $\tilde{x} = (\mathcal{E}, \tilde{Q})$ and $\tilde{x'} = (\mathcal{E}', Q')$ in $W(k)$ where $\mathcal{E}$ and $\mathcal{E}'$ are two elliptic curves over $\operatorname{Spec} W(k)$ whose special fibers are respectively isomorphic to E and E' (and $\tilde{Q}$ and $\tilde{Q'}$ are two sections of order N which specialise to Q and Q'). Let K_0 be the fraction field of $R = W(k)$. As the Picard group $\operatorname{Pic}^0_{\overline{M_1(N)}}$ is proper over the discrete valuation ring R, we have a group isomorphism

$$\operatorname{Pic}^0_{\overline{M_1(N)}}(R) \simeq \operatorname{Pic}^0_{\overline{M_1(N)}}(K_0).$$

Now we will consider the point of $\operatorname{Pic}^0_{\overline{M_1(N)}}(R)$ lifting $(x) - (x')$ corresponding to $\tilde{x}$ and $\tilde{x'}$. It is the isomorphism class of the line bundle $\mathcal{L}(\tilde{x}) \otimes \mathcal{L}(\tilde{x'})^{-1}$ where $\tilde{x}$ and $\tilde{x'}$ are $\operatorname{Spec} R$-sections of $\overline{M_1(N)}_R$ and its image in $\operatorname{Pic}^0_{\overline{M_1(N)}}(K_0)$ is the class of the divisor $((\mathcal{E}_{K_0}, \tilde{Q}) - (\mathcal{E}'_{K_0}, \tilde{Q}'))$. We can use our description of the action of T_p in characteristic 0:

$$T_p((\mathcal{E}_{K_0}, \tilde{Q}) - (\mathcal{E}'_{K_0}, \tilde{Q}')) = \sum_{H \subset \mathcal{E}[p]} (\mathcal{E}_{K_0}/H, \tilde{Q}) - \sum_{H \subset \mathcal{E}'_{K_0}[p]} (\mathcal{E}'_{K_0}/H, \tilde{Q}').$$

If $H \subset \mathcal{E}[p]$, we can show that the quotient curve $\mathcal{E}_{K_0}/H$ has good reduction over R (by thé Néron-Ogg-Shafarevich criterion for example) and let $\mathcal{E}/H$ be a model of it over $\operatorname{Spec} R$ (we could equally define $\mathcal{E}/H$ as the quotient of $\mathcal{E}$ by the finite flat subgroups scheme H and check that it is an elliptic curve over R).

By the Lemma 8.13, the finite subgroup schemes of order p in $\mathcal{E}[p]_{K_0} \subset \mathcal{E}_{K_0}$ are in bijection with the finite flat subgroup chemes of $\mathcal{E}[p]$. Consequently we have

$$T_p((\tilde{x}) - (\tilde{x}')) = \sum_{H \subset \mathcal{E}[p]} (\mathcal{E}/H, Q + H) - \sum_{H' \subset \mathcal{E}'[p]} (\mathcal{E}'/H', Q' + H')$$

where both sums are taken on finite flat subgroup schemes of order p. Finally we obtain

$$T_p((x) - (x')) = \sum_{H \subset \mathcal{E}[p]} ((\mathcal{E}/H)_k, Q + H) - \sum_{H' \subset \mathcal{E}'[p]} ((\mathcal{E}'/H')_k, Q' + H').$$

Let E be some elliptic curve defined over $k = \overline{\mathbb{F}_p}$ and assume moreover that E is ordinary. Then $E[p]$ is isomorphic, as a group scheme, with $\mu_p \times \mathbb{Z}/p\mathbb{Z}$. As μ_p is connected and its underlying space is reduced to a point, we see that $E[p]$ has only two subgroup schemes of order p : they are μ_p and $\mathbb{Z}/p\mathbb{Z}$. We have consequently to understand how many finite flat subgroup schemes of $\mathcal{E}[p]$ are reducing on μ_p or on $\mathbb{Z}/p\mathbb{Z}$. Note that, since $\mathcal{E}$ is ordinary, the group scheme structure of $\mathcal{E}[p]$ is the following : we have an extension

$$0 \to \mathcal{E}[p]^\circ \to \mathcal{E}[p] \to \mathcal{E}[p]^{\text{et}} \to 0.$$

Moreover there is a finite extension K of K_0 such that $\mathcal{E}[p]^{\text{et}}$ is isomorphic to the constant étale group $\mathbb{Z}/p\mathbb{Z}$ and $\mathcal{E}[p]^\circ$ is isomorphic to μ_p. The $\mathcal{E}[p]_{\mathcal{O}_K}$ contains exactly $p+1$ finite flat subgroups of order p. Among them, only one is connected, it is μ_p. The other one are étale and isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

First of all, we compute $(\mathcal{E}/H)_k$ when $H = \mu_p$. Since the Frobenius morphism $E \to E^{(p)}$ is not étale, its kernel is a subgroup of order p which has to be μ_p. This implies that E/μ_p is isomorphic to $E^{(p)}$, the pull back of E along the Frobenius of $\operatorname{Spec} k$. Moreover the image of the point $Q \in E[p]$ is the pullback of Q along the Frobenius and the pair $(E/\mu_p, Q + \mu_p)$ is isomorphic to the pair $(E^{(p)}, Q^{(p)})$, and it is easy to check that

$$(E^{(p)}, Q^{(p)}) - ((E')^{(p)}, (Q')^{(p)})$$

is the image of $(E, Q) - (E', Q')$ under F_* in $J(k)$.

Conversely the Verschiebung map $V : E \to E^{(p^{-1})}$ is étale and has for kernel $\mathbb{Z}/p\mathbb{Z}$. Thus if $H_k = \mathbb{Z}/p\mathbb{Z}$, we have $E/H \simeq E^{(p^{-1})}$, where $E^{(p^{-1})}$ is the elliptic curve defined on k by pullback along the inverse of the Frobenius on $\operatorname{Spec} k$ (since $\operatorname{Spec} k$ is algebraically closed the Frobenius endomorphism of $\operatorname{Spec} k$ is an automorphism). Moreover let Q_1 be the image of Q in $E/H(k)$. On the other hand, let $Q^{(p^{-1})}$ be the unique point of $E^{(p^{-1})}(k)[N]$ such that the image of $Q^{(p^{-1})}$ by the relative Frobenius $E^{(p^{-1})} \to E$ is Q. Let's recall that $F_{E^{(p^{-1})}/k} \circ V_{E/k} = [p]$ and that we use $V_{E/k}$ in order to identify E/H with $E^{(p^{-1})}$. Under this identification, we have $Q_1 = V_{E/k}(Q)$. So that $F_{E^{(p^{-1})}/k}(Q_1) = pQ$ and $F_{E^{(p^{-1})}/k}(p^{-1}Q_1) = Q$. This gives us the equality $Q^{(p^{-1})} = p^{-1}Q_1$. As

$$\begin{aligned} V((x) - (x')) &= \sum_{\substack{H \subset E[p] \\ H \ \text{étale}}} (E/H, Q^{(p^{-1})}) - \sum_{\substack{H' \subset E'[p] \\ H' \ \text{étale}}} (E'/H', (Q')^{(p^{-1})}, (Q')^{(p^{-1})}) \\ &= p((E^{(p^{-1})}, p^{-1}Q_1) - ((E')^{(p^{-1})}, p^{-1}Q_1')) \end{aligned}$$

we obtain

$$\langle p\rangle V((x)-(x')) = p((E^{(p^{-1})},Q_1)-((E')^{(p^{-1})},Q_1'))$$

and finally

$$T_p((x)-(x')) = F_*((x)-(x')) + pV_*((x)-(x'))$$

which is the desired formula. □

Remark 8.15. During the proof, in order to construct the quotient of an elliptic curve by a finite flat subgroup, we used without proof the following result.

Proposition 8.16. *Let R be a discrete valuation ring. Let E be some elliptic curve over R and H a finite flat subgroup of E. Then There exists, up to isomorphism, a unique pair (E', f) where E' is an elliptic curve over R and $f : E \to E'$ is an isogeny of kernel H.*

8.5 Some consequences

Corollary 8.17. *Let ℓ be a prime number and let p be another prime number which does not divide $N\ell$. Then the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *over* $J_1[\ell^n](\mathbb{Q})$ *is unramified the endomorphism* Frob_p *on* $J_1[\ell^n](\mathbb{Q})$ *is killed by the polynomial with coefficients in* $\mathrm{End}\, J_1(N)$

$$X^2 - T_pX + \langle p\rangle p.$$

Proof. As ℓ is different from p and p does not divide N, the finite flat group scheme $J_1(N)[\ell^n]$ is étale on $\mathrm{Spec}\,\mathbb{Z}_p$. This implies that we have a $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-equivariant isomorphism

$$J_1(N)[\ell^n](\overline{\mathbb{Q}}) = J_1(N)[\ell^n](\overline{\mathbb{Q}_p}) \simeq J_1(N)[\ell^n](\overline{\mathbb{F}_p}) \subset J_{\mathbb{F}_p}(\overline{\mathbb{F}_p}).$$

The action of Frob_p on the set on the right hand side coincides with the restriction of the endomorphism F on $J_{\mathbb{F}_p}$. However, it follows from Theorem 8.14 that we have, in $\mathrm{End}\, J_{\mathbb{F}_p}$, the factorisation

$$X^2 - T_pX + \langle p\rangle p = (X - \langle p\rangle V)(X - F).$$ □

Corollary 8.18. *Let $f \in S_2(\Gamma_1(N))$ be some normalised eigenform. Let ℓ be a prime number and λ a place of K_f dividing ℓ. Then the 2-dimensional Galois representation $\rho_{f,\lambda}$ is unramified at $p \nmid N\ell$ and*

$$\det(X - \rho_{f,\lambda}(\mathrm{Frob}_p)) = X^2 - a_p(f)X + \chi(p)p.$$

Proof. We know that the $K_{f,\lambda}$-vector space $V_\lambda(f)$ is 2-dimensional and a direct factor of $V_\lambda(f)$. Consequently the endomorphism $\rho_{f,\lambda}(\mathrm{Frob}_p)$ is killed by $X^2 - a_p(f)X + \chi(p)p$. If $\rho_{f,\lambda}(\mathrm{Frob}_p)$ is not a scalar endomorphism, we are done. If $\rho_{f,\lambda}(\mathrm{Frob}_p)$, the argument has to be completed. We won't do it here. It would require to define the Weil pairing on $J_1(N)[\ell^n]$ and to check that the adjoint of the operator F with respect to this pairing is $\langle p\rangle V$. □

We can take an explicit example. Let $f \in S_2(\Gamma_0(11)) = S_2(\Gamma_1(11))$ be the unique cuspidal normalised eigenform. Then $K_f = \mathbb{Q}$. Let $p \neq 11$ be a prime number. Then $V_p(f)$ is the Tate module of the elliptic curve $E = \overline{M_1(11)}$. The characteristic polynomial of Frob_p acting on $V_p(f)$ is $X^2 - a_p X + p$. On the other hand, since $\overline{M_1(11)}$ has good reduction outside of 11, we know that the cardinal of the finite group $E(\mathbb{F}_p)$ is $p + 1 - a_p(f)$. This shows that $a_p(f)$ is equal to

$$p - \mathrm{Card}\{(x, y) \in \mathbb{F}_p \mid y^2 + y = x^3 - x^2\}.$$

Moreover, we can deduce from Hasse Theorem that $|a_p(f)| \leqslant 2\sqrt{p}$ if $p \neq 11$. This inequality can be generalised to modular forms of arbitrary weight k (replacing $\frac{1}{2}$ by $\frac{k-1}{2}$), but we need to generalise the construction of Galois representations $V_\ell(f)$ using étale cohomology ([Del69]). The inequality is then a consequence of Weil's conjecture ([Del74], [Del80]) proved by Deligne.

References

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990.

[Con] Brian Conrad, *Inertia groups and fibers.*

[Del69] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki, no. 355, Février 1969.

[Del74] ———, *La conjecture de Weil. I.*, Publ. Math. I.H.E.S. **43** (1974), 273–307.

[Del80] ———, *La conjecture de Weil. II.*, Publ. Math. I.H.E.S. **52** (1980), 137–252.

[DG70] M. Demazure and A. Grothendieck, *Schémas en groupes. I: Propriétés générales des schémas en groupes*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151, Springer-Verlag, Berlin, 1970.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II, Lecture Notes in Math., vol. 349, 1973, pp. 143–316.

[DS] F. Diamond and J. Shurman, *A First Course in Modular Forms*, GTM, Springer.

[FK80] Hershel M. Farkas and Irwin Kra, *Riemann surfaces*, Graduate Texts in Mathematics, vol. 71, Springer-Verlag, New York-Berlin, 1980.

[Gro61a] A. Grothendieck, *Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 8, 222.

[Gro61b] ———, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11, 167.

[Gro64] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I*, Inst. Hautes Études Sci. Publ. Math. (1964), no. 20, 259.

[Gro65] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 24, 231.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52.

[KM85] N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematic Studies, no. 108, Princeton University Press, 1985.

[Mum08] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008.

[Oda69] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques, vol. 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61.

[Shi] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

[Tat74] John T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.