The modular curves $X_0(N)$.

Bas Edixhoven, Université de Rennes I.

February 2, 1999

This is a series of lectures at the ICTP Summer school on rational torsion of elliptic curves over number fields, held from 11–29 August, 1997.

Good references for the content of these lectures can be found in the recent article "Modular forms and modular curves", by Diamond and Im, in the Canadian Mathematical Society Conference Proceedings Vol. 17, "Seminar on Fermat's Last Theorem", V. Kumar Murty (editor). For example, for sections 1, 2 and 3 one can look in Shimura's book "Introduction to the arithmetic theory of automorphic forms", in Serre's "A course in arithmetic", in Lang's "Introduction to modular forms", in Miyake's "Modular forms", in Silverman's "The arithmetic of elliptic curves, in Koblitz's "Introduction to elliptic curves and modular forms", in Knapp's "Elliptic curves", etc. For sections 4 through 7, one might look in the article "Les schémas de modules des courbes elliptiques" by Deligne and Rapoport, in the book "Arithmetic moduli of elliptic curves" by Katz and Mazur, in Shimura's book mentioned above, in Gross's article "A tameness criterion for Galois representations associated to modular forms mod p", and in the article "Finiteness for the group of rational points for some modular varieties" by Kolyvagin and Logachev.

1 The Riemann surfaces $X_0(N)$ and $Y_0(N)$.

The Riemann surfaces $Y_0(N)$, for integers $N \geq 1$, are supposed to parametrize elliptic curves over $\mathbb{C}$ with given a cyclic subgroup of order N, up to isomorphism, in some sense. The $X_0(N)$ are then defined to be natural compactifications of the $Y_0(N)$. We will start with the case $N = 1$.

1.1 The Riemann surface $Y_0(1)$.

Let us recall that an elliptic curve over $\mathbb{C}$ is an irreducible non-singular complex algebraic curve of genus one, with a given point called 0. It has been shown in Mestre's lectures that such a curve can be embedded in $\mathbb{P}^2_{\mathbb{C}}$ such that the image is given by an equation of the form $y^2z = x^3+axz^2+bz^3$ and such that 0 is mapped to $(0,1,0)$. Such equations are called Weierstrass equations. A curve given by a Weierstrass equation is non-singular if and only if $4a^3 + 27b^2$ is non-zero. Conversely, every non-singular plane curve given by a Weierstrass equation with $4a^3+27b^2 \neq 0$, together with the point $(0,1,0)$, is an elliptic curve. The j-invariant of the elliptic curve given by a Weierstrass equation is defined to be $12^3 4a^3/(4a^3+27b^2)$. It was also shown in Mestre's lectures that two elliptic curves given by Weierstrass equations are isomorphic if and only if their j-invariants are the same. Therefore, the j-invariant of an elliptic curve is defined, and gives a bijection from the set $Y_0(1)$ of isomorphism classes of complex elliptic curves to $\mathbb{C}$ (it is easy to see that every z in $\mathbb{C}$ is the j-invariant of some elliptic curve). Now we want to give $Y_0(1)$ the structure of a complex analytic variety. One way to do this is to transport that structure from $\mathbb{C}$ to $Y_0(1)$, via the bijection j. We will now discuss a second way to give $Y_0(1)$ the structure of a complex analytic variety, which is easier to generalize to arbitrary N, and which will turn out to be the same.

This second method uses the complex uniformization of elliptic curves. For simplicity, we will make no distinction between complex elliptic curves (as algebraic curves) and their associated complex analytic varieties. Recall, from Mestre's lectures, that every elliptic curve E can be writen as $\mathbb{C}/\Lambda$ with Λ some lattice in $\mathbb{C}$, i.e., there exists an $\mathbb{R}$-basis (z_1, z_2) of $\mathbb{C}$ such that $\Lambda = \{az_1 + bz_2 \mid a, b \in \mathbb{Z}\}$. Moreover, for Λ_1 and Λ_2 two lattices in $\mathbb{C}$, $\mathbb{C}/\Lambda_1$ is isomorphic to $\mathbb{C}/\Lambda_2$ if and only if there exists λ in $\mathbb{C}^*$ such that $\Lambda_2 = \lambda\Lambda_1$. This allows us to parametrize the set $Y_0(1)$ as follows.

Let G be the set of group morphisms $\phi\colon \mathbb{Z}^2 \to \mathbb{C}$ such that $\phi\mathbb{Z}^2$ is a lattice, and such that ϕ gives the orientation $(i, 1)$ on the $\mathbb{R}$-vector space $\mathbb{C}$. For example, G contains the element $(a, b) \mapsto ai+b$. Then we have a surjective map from G to $Y_0(1)$, that sends ϕ to the isomorphism class of $\mathbb{C}/\phi\mathbb{Z}^2$. This map is the quotient for the two simultaneous and commuting group actions: $\mathbb{C}^*$ acts on the left on G: $\lambda\phi = (\lambda\cdot)\circ\phi$, and $\mathrm{SL}_2(\mathbb{Z})$ acts on the right on G: $\phi g = \phi\circ(g\cdot)$. Hence we have:

$$Y_0(1) = \mathbb{C}^*\backslash G/\mathrm{SL}_2(\mathbb{Z}).$$

Now view G as an open subset of $\mathbb{C}^2$ via the map sending ϕ to $(\phi(1,0), \phi(0,1))$, and let $\mathbb{H}$ be the complex upper half plane $\{z \in \mathbb{C} \,|\, \mathrm{Im}(z) > 0\}$. Then we have a bijection:

$$\mathbb{C}^* \backslash G \to \mathbb{H}, \quad \phi \mapsto \frac{\phi(1,0)}{\phi(0,1)}.$$

Moreover, we have a section from $\mathbb{H}$ to G, given by $\tau \mapsto (\tau, 1)$. It follows that we have a bijection:

$$Y_0(1) = \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}),$$

where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ by:

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

Note that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ acts trivially. Usually one finds a slightly different statement: $Y_0(1)$ is the quotient for $\mathrm{SL}_2(\mathbb{Z})$ acting on the left on $\mathbb{H}$, with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acting as $\tau \mapsto (a\tau + b)/(c\tau + d)$. Of course, both statements are equivalent, by transforming the right action into a left action via transposition $g \mapsto g^t$.

Let $p \colon \mathbb{H} \to \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ be the quotient map. Then $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ has the following structure of complex analytic variety, which makes p into a quotient morphism: a subset U of it is open if and only if $p^{-1}U$ is open in $\mathbb{H}$, a $\mathbb{C}$-valued function f on an open subset is analytic if and only if $f \circ p$ is analytic. This works because for every τ in $\mathbb{H}$ the stabilizer $\mathrm{SL}_2(\mathbb{Z})_\tau$ is finite (in fact, of order 2, 4 or 6), and every τ in $\mathbb{H}$ has an open neighborhood U such that Ug and U are disjoint if $\tau g \neq \tau$ and are equal if $\tau g = \tau$. (We will verify this in a moment.) If z is a local coordinate τ then the product of the $z \circ (\cdot g)$, for g in $\mathrm{SL}_2(\mathbb{Z})_\tau/\{1, -1\}$, is a local coordinate at $p(\tau)$. From now on we give $Y_0(1)$ this complex analytic structure.

To understand the topology of $Y_0(1)$, we construct a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. So let τ be in $\mathbb{H}$. Let z be a smallest non-zero element of $\mathbb{Z} + \mathbb{Z}\tau$. Let $\Lambda := z^{-1}(\mathbb{Z} + \mathbb{Z}\tau)$. Then $\mathbb{C}/\Lambda$ is isomorphic to $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, and 1 is a smallest non-zero element of Λ. It follows that Λ is of the form $\mathbb{Z} + \mathbb{Z}\tau'$, for a unique τ' with $-1/2 \leq \mathrm{Re}(\tau') < 1/2$, and that τ' is in $\tau\mathrm{SL}_2(\mathbb{Z})$. Since 1 is the smallest non-zero element of Λ, we have $|\tau'| \geq 1$. We define F to be the set of τ in $\mathbb{H}$ such that $-1/2 \leq \mathrm{Re}(\tau) < 1/2$, $|\tau| \geq 1$, and $|\tau| > 1$ if $\mathrm{Re}(\tau) > 0$. We claim that each $\mathrm{SL}_2(\mathbb{Z})$-orbit contains exactly one element of F. Let us first show that each orbit meets F. After the construction above, it remains to show this for the τ in $\mathbb{H}$ with $|\tau| = 1$ and $0 < \mathrm{Re}(\tau) < 1/2$. In that case, $-\tau$ is a shortest non-zero element of $\mathbb{Z} + \mathbb{Z}\tau$, and applying the construction above gives us $\tau' = -1/\tau$, which is in F. Let us now show that each orbit meets F in exactly one element. Let τ be in F, and consider the orbit of τ. Each τ' in F and in the orbit of τ arises from a shortest non-zero element z of $\mathbb{Z} + \mathbb{Z}\tau$ by the construction above. If $|\tau| > 1$, there are exactly two shortest non-zero elements, namely 1 and -1, both leading to τ. So suppose now that $|\tau| = 1$. If $\tau \neq e^{2\pi i/3}$, then there are exactly four shortest non-zero elements: 1, -1, τ and $-\tau$; these elements lead to τ, τ, $-1/\tau$ and $-1/\tau$, respectively. But $-1/\tau$ is not in F, unless $\tau = i$. Finally, if $\tau = e^{2\pi i/3}$, then there are six shortest non-zero elements: the sixth roots of unity, all of which lead to τ. We note that our computation shows moreover that the only τ in F with $\mathrm{SL}_2(\mathbb{Z})_\tau$ not equal to $\{1, -1\}$ are i and $e^{2\pi i/3}$, and that their stabilizers are cyclic of order 4 and 6, respectively, and generated by $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&-1\\1&0\end{smallmatrix}\right)$, respectively.

The existence of open neighborhoods U as claimed above can now be seen by considering F and its nine neighboring translates.

Let $\overline{F}$ be the closure of F. Then $Y_0(1)$, as a topological space, is obtained from $\overline{F}$ by some identifications on the boundary, which make it easy to see that $Y_0(1)$ is homeomorphic to $\mathbb{R}^2$. In particular, it is not compact.

Let $j\colon \mathbb{H} \to \mathbb{C}$ be the function that sends τ to the j-invariant of $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. Then j is holomorphic, and its fibres are exactly the $\mathrm{SL}_2(\mathbb{Z})$-orbits. From the universal property of the quotient morphism $p\colon \mathbb{H} \to Y_0(1)$ we get a bijective morphism of one-dimensional non-singular complex analytic varieties from $Y_0(1)$ to $\mathbb{C}$, which is then automatically an isomorphism.

Our arguments prove that, up to isomorphism, there exist exactly two complex elliptic curves E with $|\mathrm{Aut}(E)| > 2$. These two curves are $\mathbb{C}/\mathbb{Z}[i]$ and $\mathbb{C}/\mathbb{Z}[e^{2\pi i/3}]$, with automorphism groups cyclic of order four and six, respectively. They are given by the Weierstrass equations $y^2 = x^3 - x$ and $y^2 = x^3 - 1$, and have j-invariants $12^3 = 1728$ and 0, respectively.

1.2 The Riemann surfaces $Y_0(N)$.

Let us consider a complex elliptic curve $E = \mathbb{C}/\Lambda$. As a group, E is isomorphic to $\mathbb{R}/\mathbb{Z}\times\mathbb{R}/\mathbb{Z}$ (choose a $\mathbb{Z}$-basis for Λ). Let $N \geq 1$ be an integer. The kernel $E[N]$ of the multiplication by N map on E is isomorphic to $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$, or, more canonically, to $N^{-1}\Lambda/\Lambda$. We define $Y_0(N)$ to be the set of isomorphism classes of pairs (E, G), where E is a complex elliptic curve and G a cyclic subgroup of order N of E. The notion of isomorphism here is as follows: (E_1, G_1) is isomorphic to (E_2, G_2) if there exists an isomorphism $f\colon E_1 \to E_2$ such that $G_2 = f(G_1)$. We will now describe the set $Y_0(N)$ as a quotient of $\mathbb{H}$, and give it a the structure of complex analytic variety.

So let $E = \mathbb{C}/\Lambda$ be a complex elliptic curve and G a cyclic subgroup of order N. Let Λ' be the lattice containing Λ such that $\Lambda'/\Lambda = G$. Then there exists a $\mathbb{Z}$-basis (z_1, z_2) of Λ such that $(z_1, z_2/N)$ is a $\mathbb{Z}$-basis of Λ'. Multiplication by z_2^{-1} shows that (E, G) is isomorphic to $(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), \langle 1/N\rangle)$, where $\tau = z_1/z_2$ and where $\langle 1/N\rangle$ denotes the subgroup generated by the point $1/N$. This shows that we have a surjective map

$$G \to Y_0(N), \quad \phi \mapsto (\mathbb{C}/(\phi\mathbb{Z}^2), \langle\phi(0,1)\rangle).$$

This map is invariant under the left-action of $\mathbb{C}^*$ that we considered before, but, for $N > 1$, it is not invariant under all of the right-action of $\mathrm{SL}_2(\mathbb{Z})$. In fact, the subgroup that leaves it invariant is:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,|\, b \equiv 0 \bmod N \right\},$$

the inverse image under $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ of the group of lower triangular matrices. The reduction morphism from $\mathrm{SL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective, and the group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts transitively on the set of cyclic subgroups of order N of $(\mathbb{Z}/N\mathbb{Z})^2$, hence it follows that $Y_0(N)$

is the quotient of G by $\mathbb{C}^* \times \Gamma_0(N)$. So we have:

$$Y_0(N) = \mathbb{H}/\Gamma_0(N).$$

This allows us to give $Y_0(N)$ the structure of a complex analytic variety, just as we did for $Y_0(1)$ (the properties of the $\mathrm{SL}_2(\mathbb{Z})$-action that we used for this are still satisfied by all its subgroups).

By construction, $Y_0(N)$ is one-dimensional, non-singular and connected, and not compact. A fundamental domain for the $\Gamma_0(N)$-action on $\mathbb{H}$ is easy to construct, at least theoretically, because we already have the fundamental domain F for $\mathrm{SL}_2(\mathbb{Z})$. Let $g_1, \ldots, g_m$ be representatives in $\mathrm{SL}_2(\mathbb{Z})$ for $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$. Then $Fg_1 \cup \cdots \cup Fg_m$ is a fundamental domain for $\Gamma_0(N)$. Since $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$ can be identified with the set of cyclic subgroups of order N of $(\mathbb{Z}/N\mathbb{Z})^2$, and hence also with the set $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, one sees that $|\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)| = \psi(N)$, with ψ the function from positive integers to $\mathbb{Z}$ defined by $\psi(ab) = \psi(a)\psi(b)$ if a and b are relatively prime, and $\psi(p) = p + 1$ for p prime.

Let us make this more explicit for $\Gamma_0(p)$ with p prime. Then the subgroups of order p of $(\mathbb{Z}/p\mathbb{Z})^2 = \mathbb{F}_p^2$ are the $p+1$ one-dimensional $\mathbb{F}_p$-subspaces; they are generated by $(0,1)$, $(1,0)$, $(1,1), \ldots, (1, p-1)$. The elements $g_0, \ldots, g_p$ can be chosen as follows: $g_0 = 1$, $g_i = \left(\begin{smallmatrix} 0 & 1 \\ -1 & i \end{smallmatrix}\right)$ for $1 \leq i < p$. In order to make a picture of this fundamental domain F_p, it is advisable to make a picture of $F_p' := F_p \cdot \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ instead. One finds that:

$$F_p' = F \cup (F+1) \cup \cdots \cup (F+p-1) \cup F \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

It is quite easy to make the identifications on the boundary explicit. Consider, for $1 \leq a < p$ the point $a + i$. In the way we have set things up, this point corresponds to the elliptic curve $\mathbb{C}/\mathbb{Z}[i]$ with the subgroup generated by $(a+i)/p$. Multiplication by $-i$ gives an isomorphism with $(\mathbb{C}/\mathbb{Z}[i], \langle (1-ai)/p \rangle)$, which is the same as $(\mathbb{C}/\mathbb{Z}[i], \langle (b+i)/p \rangle)$ if $ab = -1$ in $\mathbb{F}_p$. This tells us how the $p-1$ arcs passing through the $a+i$ are identified. The only two remaining arcs at 0 are identified which each other.

1.3 The Riemann surfaces $X_0(N)$.

As we have already seen, the $Y_0(N)$ are not compact. In order to make the $Y_0(N)$ into algebraic objects, it is important to compactify them. Again, we begin with $Y_0(1)$. The non-compactness of $Y_0(1)$ is caused by the fact that the fundamental domain F is not bounded. So we have to study what happens "at infinity". Let $U \subset \mathbb{H}$ be the set of τ with $\mathrm{Im}(\tau) > 1$. The argument that we used to show that F is a fundamental domain also shows that two elements τ and τ' of U are in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit if and only if τ' is in $\tau + \mathbb{Z}$. Hence the map from U to $Y_0(1)$ is the quotient by the group $\mathbb{Z}$, acting by translation. But this quotient is realized by the function

$$q\colon \mathbb{H} \to \mathbb{C}, \quad \tau \mapsto e^{2\pi i \tau}.$$

Note that $qU = \{z \in \mathbb{C} \,|\, 0 < |z| < e^{-2\pi}\}$, so this punctured disk is an open subvariety of $Y_0(1)$. We compactify $Y_0(1)$ by replacing this punctured disk by the disk $\{z \in \mathbb{C} \,|\, |z| < e^{-2\pi}\}$ itself.

The resulting complex analytic variety of this procedure will be denoted by $X_0(1)$; it is by construction a compact non-singular connected one-dimensional complex analytic variety. As a topological space, it is homeomorphic to the two-sphere, hence, by the classification of compact connected non-singular one-dimensional analytic varieties, it is isomorphic to the projective line $\mathbb{P}^1(\mathbb{C})$. In fact, such an isomorphism is realized by the function j, because it has a Laurent series expansion of the form $j = q^{-1} + 744 + 196884q + \cdots$, and hence a pole of order one at the point we added. The point we added is called the cusp ∞.

Let us now consider the problem of compactifying the $Y_0(N)$. To do this, we use the morphism $f: Y_0(N) \to Y_0(1)$, and our compactification $X_0(1)$ of $Y_0(1)$. By construction, f is proper (i.e., the inverse image of a compact subset of $Y_0(1)$ is compact), and of degree $\psi(N)$. Also, we know that ramification can only occur at points with j-invariant 0 or 1728. Let D^* be the punctured disk qU described above. Then $f: f^{-1}D^* \to D^*$ is an unramified covering of degree $\psi(N)$. Up to isomorphism, the only connected unramified covering of degree n, with $n \geq 1$, of D^* is the map $D_n^* \to D^*$, with $D_n^* = \{z \in \mathbb{C} \mid 0 < |z| < e^{-2\pi/n}\}$, sending $z \mapsto z^n$. It follows that $f^{-1}D^*$ is, as a covering of D^*, a disjoint union of copies of such $D_n^* \to D^*$. Each D_n^* has the natural compactification $D_n := \{z \in \mathbb{C} \mid |z| < e^{-2\pi/n}\}$. We define $X_0(N)$ to be the compactification of $Y_0(N)$ obtained like this. The points of $X_0(N) - Y_0(N)$ are called the cusps of $X_0(N)$. By construction, the morphism $Y_0(N) \to Y_0(1)$ extends to a morphism $X_0(N) \to X_0(1)$. If we know the ramification of this morphism, we can compute the genus of $X_0(N)$ using Hurwitz's formula. So we will study the cusps in some more detail.

Recall that the stabilizer of U in $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup $\{\pm\left(\begin{smallmatrix}1&0\\n&1\end{smallmatrix}\right) \mid n \in \mathbb{Z})\}$. This is exactly the stabilizer $\mathrm{SL}_2(\mathbb{Z})_\infty$ of the point $\infty := (1,0)$ in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Z})$, for the natural right-action of $\mathrm{SL}_2(\mathbb{Z})$. In fact, the element ∞ of $\mathbb{P}^1(\mathbb{Q})$ is directly related to our fundamental domain F as follows. We can view $\mathbb{H}$ as a subset of $\mathbb{C}$, and hence as a subset of $\mathbb{P}^1(\mathbb{C})$. As such, the boundary of $\mathbb{H}$ is $\mathbb{P}^1(\mathbb{R})$, which contains $\mathbb{P}^1(\mathbb{Q})$. It turns out that the closure of F in $\mathbb{P}^1(\mathbb{C})$ meets $\mathbb{P}^1(\mathbb{R})$ exactly in the point ∞. If F_N is a fundamental domain for $\Gamma_0(N)$ acting on $\mathbb{H}$ as constructed above, then the closure of F_N in $\mathbb{P}^1(\mathbb{C})$ meets $\mathbb{P}^1(\mathbb{R})$ in the points $\infty g_1, \ldots, \infty g_{\psi(N)}$ of $\mathbb{P}^1(\mathbb{Q})$. Let g be one of the g_i. Then $\mathrm{SL}_2(\mathbb{Z})_{\infty g} = g^{-1}\mathrm{SL}_2(\mathbb{Z})_\infty g$, and hence $g\Gamma_0(N)_{\infty g}g^{-1}$ is a subgroup of finite index of $\mathrm{SL}_2(\mathbb{Z})_\infty$ containing -1, hence of the form $\{\pm\left(\begin{smallmatrix}1&0\\an&1\end{smallmatrix}\right) \mid a \in \mathbb{Z}\}$ for some unique $n \geq 1$. This means that $g\Gamma_0(N)_{\infty g}g^{-1}$ acts on U as the group of translations over $n\mathbb{Z}$. The quotient for this action is the morphism $q^{1/n}: U \to D_n^*$, sending τ to $e^{2\pi i\tau/n}$. This makes our abstract construction more explicit. It shows that the set of cusps of $X_0(N)$ is the set $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$ (use that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$). We can choose our g_i in order to have the property that if ∞g_i and ∞g_j are mapped to the same cusp in $X_0(N)$, then $\infty g_i = \infty g_j$. In this case, the cusps of $X_0(N)$ are in bijection with the points of $\mathbb{P}^1(\mathbb{Q})$ that are in the closure of F_N, and the ramification index n at a cusp of $X_0(N)$ is then simply the number of translates of F in F_N whose closure contains that cusp. A purely group theoretical description of the set of cusps of $X_0(N)$ is the set $\left(\begin{smallmatrix}1&0\\ *&1\end{smallmatrix}\right)\backslash\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$, simply because $\pm\left(\begin{smallmatrix}1&0\\ *&1\end{smallmatrix}\right)\backslash\mathrm{SL}_2(\mathbb{Z})$ is $\mathbb{P}^1(\mathbb{Q})$. But this also means that the set of cusps is the quotient set for the action of $\left(\begin{smallmatrix}1&0\\ *&1\end{smallmatrix}\right)$ on the set of cyclic subgroups of order N of $(\mathbb{Z}/N\mathbb{Z})^2$; in this description, the ramification index n of a cusp is the number of elements in the corresponding $\left(\begin{smallmatrix}1&0\\ *&1\end{smallmatrix}\right)$-orbit.

1.4 Some examples.

As an example, we will now compute, for p prime, the ramification of the morphism $f\colon X_0(p) \to X_0(1)$, and the genus of $X_0(p)$. We have already seen that f has degree $p+1$, and that it is unramified away from 0, 12^3 and ∞ (here we view $X_0(1)$ as $\mathbb{P}^1(\mathbb{C})$). The ramification over ∞ can be seen directly from the fundamental domain we constructed: $X_0(p)$ has two cusps, called 0 and ∞, the ramification indices at these cusps are p and 1, respectively.

Let us now consider the ramification over 0. The τ in $\mathbb{H}$ with $j(\tau) = 0$ form precisely the $\mathrm{SL}_2(\mathbb{Z})$-orbit of $z := e^{2\pi i/3}$, which is isomorphic, as $\mathrm{SL}_2(\mathbb{Z})$-set, with $\langle g\rangle\backslash\mathrm{SL}_2(\mathbb{Z})$, with $g := \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. It follows that the ramification over 0 is given, in the same way as at the cusps, in terms of the action of $\langle g\rangle$ on the set of one-dimensional subspaces of $\mathbb{F}_p^2$. More precisely: the set $f^{-1}(0)$ is in bijection with $\langle g\rangle\backslash\mathbb{P}^1(\mathbb{F}_p)$, and the ramification index of a point is the order of the corresponding $\langle g\rangle$-orbit. Let us now do the computation. Note that g has order three, as well as its image in $\mathrm{SL}_2(\mathbb{F}_p)$. Hence we may consider g as an element of $\mathrm{SL}_2(\mathbb{F}_p)$; its characteristic polynomial is x^2+x+1. Suppose that $p \neq 3$. Then g has two distinct eigenvalues in an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, namely the roots of unity of order three. If these roots of unity are in $\mathbb{F}_p$, then g has exactly two fixed points in $\mathbb{P}^1(\mathbb{F}_p)$ (the eigenspaces). If these roots are not in $\mathbb{F}_p$, then g has no fixed points. Whether or not the roots of unity of order three are in $\mathbb{F}_p$ is equivalent to whether or not three divides $p-1$. Suppose now that $p = 3$. Then g is conjugate to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, hence it has exactly one fixed point on $\mathbb{P}^1(\mathbb{F}_3)$. It follows that all points in $f^{-1}0$ have ramification index 3, except two of them if $p-1 \equiv 0 \bmod 3$, and except one of them if $p = 3$.

The study of the ramification over 12^3 is completely analogous to the previous arguments. One finds that all points in $f^{-1}12^3$ have ramification index 2, except two of them if $p-1 \equiv 0 \bmod 4$, and except one of them if $p = 2$.

Hurwitz's formula then tells us that the genus of $X_0(p)$ is zero if p is 2 or 3, and that it is $(p-13)/12$, $(p-5)/12$, $(p-7)/12$ or $(p+1)/12$ if $p \equiv 1$, 5, 7 or 11 mod 12, respectively.

1.5 Differential forms on $X_0(N)$.

The aim of this section is to show that holomorphic differential forms on $X_0(N)$ correspond, in a natural way, to cusp forms of weight two for the group $\Gamma_0(N)$, as defined in Frey's first lecture. So let ω be a global holomorphic 1-form on $X_0(N)$. For U an open subset of $X_0(N)$ and z a coordinate on U, we have $\omega|_U = f\,dz$ for a unique holomorphic function f on U. Let $q\colon \mathbb{H} \to Y_0(N)$ denote the quotient morphism. Then we have the 1-form $q^*\omega$ on $\mathbb{H}$. Since z is a global coordinate on $\mathbb{H}$, we have $q^*\omega = f\,dz$, for a unique holomorphic f on $\mathbb{H}$. Since q is invariant under the action of $\Gamma_0(N)$), we have, for each g in $\Gamma_0(N)$, the identity :

$$f\,dz = (\cdot g)^*(f\,dz) = (f\circ\cdot g)d(z\circ\cdot g).$$

Let us write this out for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\Gamma_0(N)$ (recall that in this text this means that $b \equiv 0 \bmod N$). The function $z\circ\cdot g$ sends τ to $(a\tau+c)/(b\tau+d)$, hence we have $z\circ\cdot g = (az+c)/(bz+d)$, and also:

$$d(z\circ\cdot g) = d\left(\frac{az+c}{bz+d}\right) = \frac{1}{(bz+d)^2}\,dz.$$

Substituting this in the identity above gives:

$$f\left(\frac{a\tau+c}{b\tau+d}\right) = (b\tau+d)^2 f(\tau), \quad \text{for all } \tau \text{ in } \mathbb{H}, \text{ and all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \text{ in } \mathrm{SL}_2(\mathbb{Z}) \text{ with } b \equiv 0 \bmod N.$$

This is exactly the invariance property for weight two modular functions on $\Gamma_0(N)$ as in Frey's first lecture.

Conversely, assume now that $f\colon \mathbb{H} \to \mathbb{C}$ is holomorphic, and satisfies the last formula. We claim that then there exists a unique holomorphic 1-form ω on $Y_0(N)$ such that $q^*\omega = f\,dz$. The existence and uniqueness of ω is clear at all points of $Y_0(N)$ at which q is an unramified cover, namely, such points have an open neighborhood U such that $q^{-1}U$ is a disjoint union of copies of U. In general, each point of $Y_0(N)$ has a neighborhood U that is isomorphic to the unit disk D, and such that $q^{-1}U$ is a disjoint union of copies of D, mapping to D via $x \mapsto x^n$, for some $n \geq 1$. Hence it suffices to analyze what happens for one such a disk. So let $n \geq 1$ and consider the morphism $q\colon D' \to D$, $x \mapsto x^n$. Let z and w be the coordinates on D and D', respectively. The morphism q is the quotient for the action of the group μ_n of nth roots of unity by multiplication on D'. A simple power series computation then shows that pulling back holomorphic 1-forms from D to D' identifies those on D with the invariant ones on D'.

At this point we know that holomorphic 1-forms on $Y_0(N)$ correspond to $\Gamma_0(N)$-invariant holomorphic 1-forms on $\mathbb{H}$, and hence to holomorphic functions on $\mathbb{H}$ satisfying the invariance property above. We would like to understand, in terms of functions on $\mathbb{H}$, what it means that a 1-form on $Y_0(N)$ is holomorphic at the cusps. Let us first describe the situation at the cusp ∞. Let ω be a 1-form on $Y_0(N)$ and let f be defined by $q^*\omega = f\,dz$. Then we have $f(\tau+1) = f(\tau)$ for all τ in $\mathbb{H}$, because $\Gamma_0(N)$ contains $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Hence f is a Laurent series in $q = e^{2\pi i z}$, i.e., $f = \sum_{n\in\mathbb{Z}} a_n q^n$, for certain a_n in $\mathbb{C}$. Note that $2\pi i\,dz = q^{-1}\,dq$, and recall that q is the coordinate of the disk of which ∞ is the center. The identity:

$$f\,dz = \frac{1}{2\pi i}\sum_{n\in\mathbb{Z}} a_n q^n \,\frac{dq}{q}$$

shows that ω is holomorphic at ∞ if and only if $a_n = 0$ for all $n \leq 0$. The situation at the other cusps of $X_0(N)$ is similar. If one goes back to our compactification procedure, one sees that ω is holomorphic at all the cusps, if and only if for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$, the function:

$$\tau \mapsto \frac{1}{(b\tau+d)^2}\, f\left(\frac{a\tau+c}{b\tau+d}\right)$$

from $\mathbb{H}$ to $\mathbb{C}$ has its Laurent series expansion in $q^{1/n}$, where n is the ramification index of the cusp $\infty\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, of the form $\sum_{m\geq 1} a_m q^{m/n}$. This means that the holomorphic 1-forms on $X_0(N)$ are precisely the cusp forms of weight two on $\Gamma_0(N)$ as defined in Frey's lecture. As a consequence, it follows that the dimension of the space $S_2(\Gamma_0(N))$ is equal to the genus of $X_0(N)$.

2 Hecke correspondences.

The aim of this section is to give a geometric interpretation, in terms of 1-forms on $X_0(N)$, of the Hecke operators, degeneracy maps and Atkin-Lehner involutions on $S_2(\Gamma_0(N))$ defined in Frey's second lecture.

2.1 Degeneration morphisms.

Let N, M and r be positive integers, such that rM divides N. We will define a map $B_{N,M,r}$, also denoted B_r, from the set $Y_0(N)$ to the set $Y_0(M)$. After that we will show that it is a morphism of complex analytic varieties, that extends to a morphism B_r from $X_0(N)$ to $X_0(M)$. Recall that $Y_0(N)$ is the set of isomorphism classes of pairs (E,G), with E a complex elliptic curve and $G\subset E$ a cyclic subgroup of order N. To such a pair we associate the pair $(E/G[r],\overline{G}[M])$, where $G[r]$ denotes the kernel of multiplication by r in G, and where $\overline{G}$ denotes the image of G in $E/G[r]$. The pair $(E/G[r],\overline{G}[M])$ defines a point of $Y_0(M)$, since $\overline{G}[M]$ is indeed cyclic of order M. The definition is clearly compatible with isomorphisms of pairs (E,G), hence we have indeed defined our map B_r from $Y_0(N)$ to $Y_0(M)$. Let us now verify that this map is a morphism of complex analytic varieties. For this we will use the universal property of the quotient morphisms $\mathbb{H}\to Y_0(N)$ and $\mathbb{H}\to Y_0(M)$. So let τ be in $\mathbb{H}$. The image of τ in $Y_0(N)$ is the isomorphism class of $(E,G)=(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau),\langle 1/N\rangle)$. The group $G[r]$ is generated by $1/r$, hence $E/G[r]$ is $\mathbb{C}/(\mathbb{Z}\ 1/r+\mathbb{Z}\tau)$, and the subgroup $\overline{G}[M]$ is generated by $1/rM$. Multiplication by r on $\mathbb{C}$ induces an isomorphism from $(E/G[r],\overline{G}[M])$ to $(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}r\tau),\langle 1/M\rangle)$. It follows that we have a commutative diagram:

$$\begin{array}{ccc} \mathbb{H} & \to & \mathbb{H} \\ \downarrow & & \downarrow \\ Y_0(N) & \to & Y_0(M) \end{array}$$

in which the map from $\mathbb{H}$ to $\mathbb{H}$ is multiplication by r, in which the vertical arrows are the quotient morphisms, and in which the map from $Y_0(N)$ to $Y_0(M)$ is B_r. The universal property of the quotient morphism $\mathbb{H}\to Y_0(N)$ implies that B_r is a morphism. Let us now argue that B_r extends to a morphism from $X_0(N)$ to $X_0(M)$. The automorphism "$\cdot r$" of $\mathbb{H}$ is induced by the element $\left(\begin{smallmatrix} r & 0 \\ 0 & 1\end{smallmatrix}\right)$ of $\mathrm{GL}_2(\mathbb{R})^+$ (the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is in fact the restriction of the action of $\mathrm{GL}_2(\mathbb{R})^+$ on it). Via this isomorphism, the action of $\Gamma_0(N)$ on $\mathbb{H}$ becomes the action of its conjugate $\Gamma := \left(\begin{smallmatrix} r & 0 \\ 0 & 1\end{smallmatrix}\right)^{-1}\Gamma_0(N)\left(\begin{smallmatrix} r & 0 \\ 0 & 1\end{smallmatrix}\right)$, which is a subgroup of $\Gamma_0(M)$ (it is in fact the subgroup of $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbb{Z})$ with $c\equiv 0 \bmod r$ and $b\equiv 0 \bmod N/r$). So $\cdot r$ induces an isomorphism from $Y_0(N)$ to $\mathbb{H}/\Gamma$. The compactification procedure that we used for $\Gamma_0(N)$ works in fact for all subgroups of finite index of $\mathrm{SL}_2(\mathbb{Z})$, hence also for Γ, and one can see that $\cdot r$ extends to an isomorphism from $X_0(N)$ to $\overline{\mathbb{H}/\Gamma}$, and that the canonical morphism from $\mathbb{H}/\Gamma$ to $Y_0(M)$ extends to a morphism from $\overline{\mathbb{H}/\Gamma}$ to $X_0(M)$.

The morphism B_r gives, by pullback, a map from the space of holomorphic 1-forms $\Omega(X_0(M))$

on $X_0(M)$ to $\Omega(X_0(N))$. Let ω be in $\Omega(X_0(M))$, and write $q_M^*\omega = \sum_{n\geq 1} a_n q^n\, dq/q$, where q_M is the quotient map from $\mathbb{H}$ to $Y_0(M)$. Then $B_r^*(\omega)$ is determined by: $q_N^* B_r^*\omega = r\sum_{n\geq 1} a_n q^{nr}\, dq/q$.

On the other hand, B_r also gives, by a kind of trace map, a map from $\Omega(X_0(N))$ to $\Omega(X_0(M))$. The easiest way to describe that map in our context is as follows. Let ω be in $\Omega(X_0(N))$, let ω_1 be its pullback to $\mathbb{H}$, and let ω_2 be the 1-form it gives on $\mathbb{H}$ via the isomorphism $\cdot r$; then ω_2 is Γ-invariant. Let $g_1,\ldots,g_n$ be representatives for $\Gamma_0(M)/\Gamma$. Then $g_1\omega_2+\cdots+g_n\omega_2$ is $\Gamma_0(M)$-invariant, and corresponds to an element $B_{r*}\omega$ of $\Omega(X_0(M))$. A quite different way to describe the map B_{r*} is as follows. Let U be a small open subset of $X_0(M)$, with a coordinate z. Then the $\mathbb{C}$-algebra $\mathcal{O}(B_r^{-1}U)$ of holomorphic functions on $B_r^{-1}U$ is free of rank the degree of B_r as a module over $\mathcal{O}(U)$. This gives us a trace map $\mathrm{tr}\colon \mathcal{O}(B_r^{-1}U)\to\mathcal{O}(U)$. Let ω be an element of $\Omega(B_r^{-1}U)$, and write it as $f\,d(z\circ B_r)$, with f meromorphic on $B_r^{-1}U$. Then $B_{r*}\omega = \mathrm{tr}(f)\,dz$ on U. There is probably not a simple formula for $B_{r*}\omega$ just in terms of the q-expansion of ω because of the g_i in the first description, or, equivalently, because there is in general more than one cusp of $X_0(N)$ mapped by B_r to the cusp ∞ of $X_0(M)$.

2.2 Atkin-Lehner involutions.

Let $N\geq 1$ be an integer, and $r\geq 1$ a divisor of N such that r and N/r are relatively prime. Let x be a point of $Y_0(N)$, say the isomorphism class of a pair (E,G). Then to (E,G) we associate the pair $w_r(E,G) := (E/G[r], \overline{E[r]+G})$, giving a point $w_r(x)$ of $Y_0(N)$. This construction defines a map w_r from $Y_0(N)$ to itself. Multiplication by r on E gives an isomorphism between (E,G) and $w_r(w_r(E,G))$ (to see this, it is useful to note that G is the direct sum of $G[r]$ and $G[N/r]$). Therefore, w_r is an involution of the set $Y_0(N)$, called an Atkin-Lehner involution. Note that the set of divisors r of N such that r and N are relatively prime form a boole algebra with 2^n elements, where n is the number of prime numbers dividing N. It is easy to verify that the w_r commute among each other, and that the group they generate is the additive group of the boole algebra just mentioned. To be explicit: $w_r w_s = w_{\mathrm{lcm}(r,s)/\gcd(r,s)}$.

We will now prove that w_r is an automorphism of the complex analytic variety $Y_0(N)$, and that as such it extends to $X_0(N)$. The strategy is the same as for the B_r. So let τ be in $\mathbb{H}$, and (E,G) the pair associated to τ, i.e., $E=\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ and $G=\langle 1/N\rangle$. Then $G[r]=\langle 1/r\rangle$, hence $E/G[r] = \mathbb{C}/(\mathbb{Z}\,1/r+\mathbb{Z}\tau)$, and $\overline{E[r]+G} = \langle \tau/r+1/N\rangle$ (note that τ/r and $1/N$ have order r and N/r, respectively, in $E/G[r]$. We define:

$$\tau_1 := N(\tau/r+1/N) = (N/r)\tau + r(1/r).$$

Choose integers a and b such that $ar - b(N/r) = 1$, and define $\tau_2 := a\tau + b(1/r)$. Then τ_1 and τ_2 form a $\mathbb{Z}$-basis for $\mathbb{Z}\,1/r+\mathbb{Z}\tau$, and division by τ_1 shows that $w_r(E,G)$ is isomorphic to $(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau'), \langle 1/N\rangle)$, with $\tau' = \tau_2/\tau_1 = \tau\left(\begin{smallmatrix} ar & N\\ b & r\end{smallmatrix}\right) = \tau\left(\begin{smallmatrix} r & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} a & N/r\\ b & r\end{smallmatrix}\right)$. Let $g := \left(\begin{smallmatrix} ar & N\\ b & r\end{smallmatrix}\right)$; the fact that the image of τg in $Y_0(N)$ is well-defined implies that g normalizes $\Gamma_0(N)$ (one can verify this via a silly matrix computation, but, of course, one doesn't need to). Form this it follows that $\cdot g$ defines an automorphism of $Y_0(N)$, which is, by construction, w_r, and it follows that w_r extends to an automorphism of $X_0(N)$. This finishes the proof that w_r is an involution of the complex analytic variety $X_0(N)$.

Since the w_r do not necessarily fix the cusp ∞, one cannot expect to have simple formulas in terms of q-expansions for their action on $\Omega(X_0(N))$. It is certainly possible to describe all relations between degeneracy maps and Atkin-Lehner involutions, but I don't see the need to do it at this moment.

2.3 Hecke correspondences.

As we have seen above, there are many morphisms among the curves $X_0(N)$, along which one can push and pull differential forms. One way to exploit the existence of all the induced maps among the $\Omega(X_0(N))$ is to say that all these maps come in some sense from the action of $\mathrm{SL}_2(\mathbb{Q})$ on $\mathbb{H}$, and to consider the action on the direct limit of the $\Omega(X)$, where X ranges over through the system of all modular curves. This leads to using the representation theory of $\mathrm{SL}_2(\hat{\mathbb{Z}}\otimes\mathbb{Q})$. This point of view is very important in order to understand the details of the relations between modular forms and Galois representations. However, we will not take this point of view in these lectures, for the simple reason that we need to know some other kind of properties of $X_0(N)$ and its jacobian variety.

The fact that the $\Gamma_0(N)$-action on $\mathbb{H}$ is in fact the restriction of an action of $\mathrm{GL}_2(\mathbb{R})^+$ leads, by a completely group theoretical construction involving the set $\Gamma_0(N)\backslash\mathrm{GL}_2(\mathbb{Q})^+/\Gamma_0(N)$ of double cosets, to certain operators T_n $(n\geq 1)$, called Hecke operators, on $\Omega(X_0(N))$. A more direct and useful way for us will be to construct these operators via the modular interpretation of $Y_0(N)$, and isogenies between elliptic curves.

Let us fix $N\geq 1$. For each $n\geq 1$ and $x=(E,\langle P\rangle)$ in $Y_0(N)$ we define:

$$T_n(x) := \sum_G (E/G, \langle\overline{P}\rangle),$$

where G runs through the set of subgroups of order n of E that have trivial intersection with $\langle P\rangle$. By definition, $T_n(x)$ is an element of the $\mathbb{Z}$-module $\mathrm{Div}(Y_0(N))$ of divisors on $Y_0(N)$. It is clear that T_n extends in a unique way to an endomorphism of $\mathrm{Div}(Y_0(N))$. As such, it multiplies the degree of divisors by an integer that is easily computed. For example, for p prime, T_p multiplies the degree by $p+1$ if p does not divide N, and by p if p divides N. Our next objective is to show that the T_n are in fact holomorphic correspondences that extend to $X_0(N)$, and to study their action on $\Omega(X_0(N))$. To do that, it is a good idea to express all T_n in terms of the T_p with p prime. It is a good exercise to show that:

$$T_nT_m = T_{nm} \quad \text{if } \gcd(n,m)=1,$$

and that for p prime:

$$T_pT_{p^r} = \begin{cases} T_{p^{r+1}} & \text{if } p \text{ divides } N \\ T_{p^{r+1}} + pT_{p^{r-1}} & \text{if } p \text{ does not divide } N. \end{cases}$$

These identities imply that the T_p with p prime generate all T_n, that all T_n commute among each other, and that one has the following identity of formal Dirichlet series:

$$\sum_{n\geq 1} T_n n^{-s} = \prod_{p|N}(1-T_pp^{-s})^{-1}\prod_{p\nmid N}(1-T_pp^{-s}+p^{1-2s})^{-1}.$$

In order to show that the T_n are holomorphic correspondences, it is now enough to show it for the T_p with p prime. So let p be a prime, and x in $Y_0(N)$. Pick τ in $\mathbb{H}$ such that x is the image of τ under the quotient map. Then $x = (\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), \langle 1/N\rangle)$. Recall that $E[p]$ has $\mathbb{F}_p$-basis $1/p$, τ/p. Hence the possible subgroups G of order p are $\langle 1/p\rangle$ if p does not divide N, and the $\langle(\tau+i)/p\rangle$ for $0 \leq i < p$. It follows that $T_p(x)$ is the image of $p\tau + \sum_i(\tau+i)/p$ if p does not divide N, and of $\sum_i(\tau+i)/p$ if p divides N. In other words, T_p is induced by the operator:

$$T_p\colon \tau \mapsto \begin{cases} p\tau + \sum_{0\leq i<p}(\tau+i)/p & \text{if } p \text{ does not divide } N \\ \sum_{0\leq i<p}(\tau+i)/p & \text{if } p \text{ divides } N. \end{cases}$$

It follows from this that $T_p(x) = B_1 B_p^{-1}(x)$, whether p divides N or not. In other words, T_p extends to the holomorphic correspondence:

$$\begin{array}{ccc} & X_0(pN) & \\ {}^{B_p}\swarrow & & \searrow^{B_1} \\ X_0(N) & & X_0(N) \end{array}$$

If p does not divide N, then $B_p = B_1 \circ w_p$, which shows that in that case T_p is a symmetric correspondence.

We let the T_n act on $\Omega(X_0(N))$ via pullback, i.e., as $B_{p*}\circ B_1^*$. The formula above for $T_p\tau$ then gives the result that for $\omega = \sum a_n q^n\, dq/q$ in $\Omega(X_0(N))$ one has

$$T_p\omega = \begin{cases} \sum(pa_{n/p} + a_{np})q^n\, dq/q & \text{if } p \text{ does not divide } N \\ \sum(a_{np})q^n\, dq/q & \text{if } p \text{ does divide } N, \end{cases}$$

with the convention that $a_{n/p} = 0$ if n/p is not an integer. Combining the formulas above, one can finally obtain the following result: for $\omega = \sum a_n q^n\, dq/q$ in $\Omega(X_0(N))$ and $m \geq 1$, one has $T_m(\omega) = \sum b_n q^n\, dq/q$, with:

$$b_n = \sum_{\substack{d|(n,m) \\ (d,N)=1}} d\, a_{nm/d^2}.$$

In particular, we have, in the notation above:

$$b_1 = a_m,$$

which implies that if ω is an eigenform for all T_m, say with eigenvalues λ_m, then $a_n = \lambda_n a_1$ for all n. Hence the common eigenspaces for the T_n acting on $\Omega^1(X_0(N))$ have dimension one.

3 The $X_0(N)$ as complex algebraic curves.

Every compact Riemann surface is the analytic variety associated to some projective algebraic curve. In the case of the $X_0(N)$ we will make this a bit more explicit.

3.1 General results for compact Riemann surfaces.

In order to be precise, we have to say what we will mean by a complex algebraic variety. So here is our definition, which is very close to the one in Serre's "Faisceaux algébriques cohérents".

3.1.1 Definition. *A complex algebraic variety is a pair $(X, \mathcal{O}_X)$ with X a topological space, $\mathcal{O}_X$ a sheaf of $\mathbb{C}$-valued functions on X, such that X has a cover by open subsets U such that $(U, \mathcal{O}_X|_U)$ is isomorphic to some pair $(Z, \mathcal{O}_Z)$ with Z a Zariski closed subset of $\mathbb{C}^n$ for some n, endowed with the Zariski topology and the sheaf $\mathcal{O}_Z$ of regular functions. The notion of isomorphism here means that there is a homeomorphism $\phi: U \to Z$ under which the regular functions on open subsets of Z correspond to the functions in $\mathcal{O}_X$. A morphism of complex algebraic varieties $f: X \to Y$ is a continuous map such that for all $U \subset Y$ open and g in $\mathcal{O}_Y(U)$, $g \circ f$ is in $\mathcal{O}_X(f^{-1}U)$.*

We can now describe how one associates, to a complex algebraic variety X, a complex analytic variety X^{an}. As a set, X^{an} is just X. A subbasis for the topology of X^{an} is given by sets U that one obtains as follows: take a Zariski open subset V of X, and a regular function f on V, then $U := \{x \in V \mid |f(x)| < 1\}$. Finally, the analytic functions are those that can locally be written as a power series in a finite number of regular functions. This construction is clearly a functor. If X is a non-singular complex algebraic curve, then X^{an} is a Riemann surface, which is compact if X is projective. Serre's GAGA theory says that the functor $X \mapsto X^{\mathrm{an}}$ gives an equivalence between the projective varieties on both sides.

The theorem of Riemann-Roch implies that every compact Riemann surface is projective, hence the GAGA theory says that category of compact Riemann surfaces is equivalent to that of non-singular projective complex algebraic curves. Hence to a compact Riemann surface X one can associate a projective algebraic curve X^{alg}. Let us describe explicitly how this works. As a set, X^{alg} is X. The topology of X^{alg} is the Zariski topology: the open sets are the cofinite sets, and the empty set. The regular functions on a non-empty Zariski open set U are the holomorphic functions on U that extend to a meromorphic function on X. In order to prove that the pair $(X^{\mathrm{alg}}, \mathcal{O})$ just defined is in fact a non-singular projective algebraic curve, one proceeds as follows. One first reduces to the case where X is connected. Let $U \subset X$ be Zariski open, not empty, and not X itself. By Riemann-Roch, there exists a surjective morphism $f: X \to \mathbb{P}^1(\mathbb{C})$ such that $U = f^{-1}\mathbb{C}$. Using Riemann-Roch again, one shows that $\mathcal{O}(U)$ is a finitely generated $\mathbb{C}[f]$-module. It follows that $\mathcal{O}(U)$ is integral over $\mathbb{C}[f]$ and that the function field $\mathbb{C}(X)$ of meromorphic functions on X is of the form $\mathbb{C}(f, g)$ with g algebraic over $\mathbb{C}(f)$. Then one proceeds to show that X^{alg} is the non-singular algebraic curve that corresponds to the function field $\mathbb{C}(X)$. For example, for P in U one can take g in $\mathcal{O}(U)$ such that g has a simple zero at P and no zero at the other points in the fibre of P under f; then f and g define a morphism from X^{alg} to $\mathbb{P}^1_{\mathbb{C}}\times\mathbb{P}^1_{\mathbb{C}}$ that gives a closed immersion over a neighborhood of $(f(P),0)$.

3.2 The case $X_0(N)$.

For $X_0(N)$ one can make the construction at the end of the previous section more explicit, using the two degeneracy morphisms B_1 and B_N from $X_0(N)$ to $X_0(1)=\mathbb{P}^1(\mathbb{C})$. So let $j_1:=j{\circ}B_1$ and $j_N:=j{\circ}B_N$; j_1 and j_N are then meromorphic functions on $X_0(N)$. Let us show that these two functions generate $\mathbb{C}(X_0(N))$. Let Φ_N in $\mathbb{C}(j_1)[y]$ be the minimum polynomial of j_N over $\mathbb{C}(j_1)$. We know that the degree of B_1 is $\psi(N)$, so we have to show that Φ_N has degree $\psi(N)$. For that it is enough to find one elliptic curve E over $\mathbb{C}$ such that $j_1^{-1}(j(E))$ has exactly $\psi(N)$ elements, on which j_N takes distinct values. Let us take E such that the endomorphism ring of E is $\mathbb{Z}$ (for example, take $E=\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ with τ in $\mathbb{H}$ not quadratic over $\mathbb{Q}$). Then, first of all, E has automorphism group $\{1,-1\}$, hence its number of cyclic subgroups G of order N, up to isomorphism, is exactly $\psi(N)$. The values of j_N on $j_1^{-1}(j(E))$ are the $j(E/G)$. Suppose now that G_1 and G_2 are two cyclic subgroups of order N of E, and that $\sigma\colon E/G_1\to E/G_2$ is an isomorphism. Let p_1 and p_2 be the quotient morphisms from E to E/G_1 and E/G_2, and let q_2 be the morphism from E/G_2 to E such that $q_2{\circ}p_2=N$. Then $q_2{\circ}\sigma{\circ}p_1$ is an endomorphism ϕ of E, hence multiplication by some integer. Since ϕ has degree N^2, $\phi=\pm N$. After replacing σ by $-\sigma$, if necessary, we have $\phi=N$. But then $q_2{\circ}\sigma{\circ}p_1=q_2{\circ}p_2$, which implies that $\sigma{\circ}p_1=p_2$ (since the kernel of q_2 is finite, and E connected). Hence $G_1=G_2$. We have now proved that $\mathbb{C}(X_0(N))=\mathbb{C}(j_1,j_N)$.

The reader is referred to Oesterlé's notes for proofs of the following statements:

1. j_N is integral over $\mathbb{C}[j_1]$,

2. the morphism $(j_1,j_N)\colon Y_0(N)\to\mathbb{C}^2$ sends $P=(E,G)$ to a singular point of the curve Y defined by Φ_N if and only if E has an endomorphism of degree N^2, whose kernel contains G and is not $E[N]$,

3. Φ_N is in $\mathbb{Z}[x,y]$, symmetric, and irreducible in $\mathbb{C}[x,y]$,

4. $Y_0(N)^{\mathrm{alg}}$ is the normalization of Y.

4 $X_0(N)$ over $\mathbb{Z}[1/N]$ and its moduli interpretation.

The fact that the Φ_N are actually polynomials with coefficients in $\mathbb{Z}$ shows that the $X_0(N)_{\mathbb{C}}$, the complex algebraic curves associated to the Riemann surfaces $X_0(N)$, are naturally defined over $\mathbb{Q}$. More precisely, we will say that a model over $\mathbb{Q}$ of a complex algebraic variety X is a variety Y over $\mathbb{Q}$ (which is for us a $\mathbb{Q}$-scheme of finite type that is separated and reduced), together with an isomorphism from $Y_{\mathbb{C}}$ to X, where $Y_{\mathbb{C}}$ denotes the complex algebraic variety obtained from Y by extending scalars from $\mathbb{Q}$ to $\mathbb{C}$. Let Y_N be the closed subvariety $\mathbb{P}^1_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}}$ that is defined by Φ_N, and let $X_0(N)_{\mathbb{Q}}$ be the normalization of Y_N. Then $X_0(N)_{\mathbb{Q}}$, with the natural isomorphism from $(X_0(N)_{\mathbb{Q}})_{\mathbb{C}}$ to $X_0(N)_{\mathbb{C}}$, is a model over $\mathbb{Q}$ of $X_0(N)_{\mathbb{C}}$. In the same way, one obtains a model $X_0(N)_{\mathbb{Z}}$ over $\mathbb{Z}$. This definition of the $X_0(N)_{\mathbb{Q}}$ is good enough to study rationality questions of points and of morphisms between the $X_0(N)_{\mathbb{Q}}$; this is the point of view taken in Oesterlé's notes. However, in the end we will want to know that $X_0(N)_{\mathbb{Z}}$ has good reduction at all primes not dividing N. In order to prove such results, it is more convenient to have a better interpretation of $X_0(N)_{\mathbb{Z}}$, say at least over $\mathbb{Z}[1/N]$, as a moduli space. This is the point of view that we will take in the lectures that follow. Unfortunately, in order to even define what a moduli space is, we have to be more technical than we have been until now. In particular, we will use the language of schemes, categories and functors.

4.1 The main categories and functors.

We denote by Sch the category of schemes. People who are afraid of schemes can keep in mind that a scheme is just something that one obtains by glueing affine schemes, and that the category of affine schemes is anti-equivalent to the category of commutative rings, and that all commutative rings are of the form $\mathbb{Z}$[generators]/relations.

For a scheme S, we let Sch/S be the category of S-schemes, i.e., the objects are schemes X together with a morphism $f\colon X \to S$, and a morphism from $f\colon X \to S$ to $g\colon Y \to S$ is a morphism of schemes $h\colon X \to Y$ that is compatible with f and g.

Let S be a scheme, and X an S-scheme. We define a contravariant functor $h_X\colon \mathrm{Sch} \to \mathrm{Set}$ as follows. For any S-scheme T, we put $h_X(T) = \mathrm{Hom}_S(T, X)$, the set of morphisms from T to X in Sch/S; we will also denote this set by $X(T)$, and call it the set of T-valued points of X/S. For $f\colon T_1 \to T_2$ a morphism of S-schemes, $h_X(f)$ sends g in $X(T_2)$ to $g \circ f$ in $X(T_1)$.

For example, let $S := \mathrm{Spec}(\mathbb{Q})$, $X := \mathrm{Spec}(\mathbb{Q}[x,y]/(x^n + y^n - 1))$, for some n, and $T := \mathrm{Spec}(A)$ with A a $\mathbb{Q}$-algebra. Then $X(A) := X(T)$ is the set of pairs (a, b) with a and b elements of A satisfying $a^n + b^n = 1$.

Another example that shows that this functorial point of view is useful is as follows. Let again S be a scheme. A group scheme G over S is then nothing else but an S-scheme G, together with a factorization of the functor $h_G\colon \mathrm{Sch}/S \to \mathrm{Set}$ through the forget functor from the category of groups Grp to Set. In more simple terms, this means that every $G(T)$ has been given the structure of a group, in a compatible way for varying T.

Of course, this kind of construction, associating h_X to X, can be done for arbitrary categories. A fundamental and trivial result (Yoneda's lemma) about this construction is that for $\mathcal{C}$ a category, $h: X \mapsto h_X$ defines a fully faithful covariant functor from $\mathcal{C}$ to the category $\tilde{\mathcal{C}}$ of contravariant functors from $\mathcal{C}$ to Set. In other words, h identifies $\mathcal{C}$ with a full subcategory of $\tilde{\mathcal{C}}$. The $F: \mathcal{C} \to \mathrm{Set}$ in $\tilde{\mathcal{C}}$ that are isomorphic to some h_X with X in $\mathcal{C}$ are called the representable functors. A detailed discription of this matter can be found at the beginning of EGA 1 (the Springer-Verlag edition).

Before we go back to our schemes, one more generality concerning fibered products. Let $f: X \to S$ and $g: Y \to S$ be morphisms in some category $\mathcal{C}$. A fibered product of f and g is then a triple (Z, f', g'), with $f': Z \to Y$ and $g': Z \to X$, such that $f \circ g' = g \circ f'$, such that if (Z', f'', g'') also is such a triple, then there exists a unique $h: Z' \to Z$ with $f' \circ h = f''$ and $g' \circ h = g''$. Fibered proucts do not always exist, but if one exists, it is unique up to unique isomorphism, and denoted $(X \times_X Y, p_X, p_Y)$; p_X and p_Y are called the projections to X and Y. If S is a final object, then $X \times_S Y$ is called the product of X and Y, and is denoted $X \times Y$. It is a good exercise to show that $h_{X \times_S Y} = h_X \times h_Y$.

For the following fundamental results on elliptic curves over arbitrary schemes, the book "Arithmetic moduli of elliptic curves" by Katz and Mazur, provides an excellent reference.

4.1.1 Definition. *Let S be a scheme. An elliptic curve E over S is then a proper smooth curve with geometrically connected fibres of genus one, together with a point 0 in $E(S)$.*

For $f: E \to S$ an elliptic curve, we define $\mathrm{Pic}^0(E)$ to be the subgroup of $\mathrm{Pic}(E)$ consisting of isomorphism classes of invertible $\mathcal{O}_E$-modules $\mathcal{L}$ whose restrictions to the fibres of E/S have degree zero. We define $\mathrm{Pic}^0(E/S)$ to be $\mathrm{Pic}^0(E)/f^*\mathrm{Pic}(S)$.

4.1.2 Proposition. *Let E be an elliptic curve over a scheme S. For every S-scheme T the map from $E(T) = E_T(T)$ to $\mathrm{Pic}^0(E_T/T)$ that sends P to the class of $I(P_T)^{-1} \otimes I(0)$ is a bijection.*

It follows that $E(T)$ has the structure of abelian group, functorially in T. Hence E/S is an abelian group scheme.

4.1.3 Proposition. *Let E/S be an elliptic curve. Then, Zariski locally on S, E/S can be embedded in $\mathbb{P}^2_S$, with the image given by a Weierstrass equation. All the formulas of Mestre's lectures concerning $a_1, \ldots, a_6$, etc., are valid in this context. In particular, the properties of Δ show that the invertible $\mathcal{O}_S$-module $(0^*\Omega^1_{E/S})^{\otimes 12}$ is canonically trivial.*

4.1.4 Remark. Let S be a scheme and E/S an elliptic curve. A necessary condition for E/S to be given by a Weierstrass equation is that the invertible $\mathcal{O}_S$-module $0^*\Omega^1_{E/S}$ be trivial. Suppose that this is so. Then, if S is affine, or if 6 is invertible on S, E/S does admit a Weierstrass equation. I do not know whether every elliptic curve E/S with trivial $0^*\Omega^1_{E/S}$ admits a Weierstrass equation. □

A morphism of schemes $f: X \to Y$ is called finite if for every affine open $\mathrm{Spec}(A)$ of Y the inverse image $f^{-1}\mathrm{Spec}(A)$ is affine, say $\mathrm{Spec}(B)$, with B an A-module of finite type. A finite morphism $f: X \to Y$ is called locally free if for all A and B as above, B is locally free as

A-module. A morphism $f: X \to Y$ is called finite etale if it is finite, locally free, and has geometrically reduced fibres (this last condition is equivalent to saying that $\Omega^1_{X/Y} = 0$). If A is a local ring, and B is a local A-algebra, then B is finite etale over A if and only if it is of the form $A[x]/(f)$, with f monic, and irreducible and separable over the residue field of A. For example, if A is local and complete, with separably closed residue field, then the finite etale A-algebras are the A^n, $n \geq 0$.

4.1.5 Proposition. *Let E/S be an elliptic curve. For n in $\mathbb{Z}$ let $[n]: E \to E$ be the map that sends P to nP in the group law. Let $n \neq 0$. Then $[n]$ is finite and locally free of rank n^2. If n is invertible on S, then the kernel $E[n] = \ker([n]) = S \times_E E$ (with $E \to E$ given by $[n]$) is finite étale over S, and, after a suitable surjective finite etale base change $T \to S$, isomorphic to the group scheme $(\mathbb{Z}/n\mathbb{Z})^2_T$.*

4.1.6 Definition. *Let $N \geq 1$. A $\Gamma_0(N)$-structure on elliptic curve E over a $\mathbb{Z}[1/N]$-scheme S is a subgroup scheme G of E which is, after a suitable surjective finite etale base change $T \to S$, isomorphic to $(\mathbb{Z}/N\mathbb{Z})_T$. For S a $\mathbb{Z}[1/N]$-scheme, let $F_N(S)$ be the set of isomorphism classes of pairs $(E/S, G)$, where E is an elliptic curve over S and G a $\Gamma_0(N)$-structure on E/S. For $f: S' \to S$, let $F_N(f): F_N(S) \to F_N(S')$ be the map given by base change via f. Then $F_N: \mathrm{Sch}/\mathbb{Z}[1/N] \to \mathrm{Set}$ is a contravariant functor.*

4.2 $X_0(N)_{\mathbb{Z}[1/N]}$ as a coarse moduli space.

A natural way to demand that a $\mathbb{Z}[1/N]$-scheme X parametrizes elliptic curves with a cyclic subgroup of order N is to ask for an isomorphism of functors $F_N \to h_X$, since this would mean that over X there is a universal pair $(E_{\mathrm{univ}}, G_{\mathrm{univ}})$ from which every (E, G) is obtained by base change via a unique morphism $S \to X$. In that case, X, together with $(E_{\mathrm{univ}}, G_{\mathrm{univ}})$, would be called a fine moduli space. Unfortunately, such X do not exist, for any N. This is due to the fact that the objects we are classifying have non-trivial automorphisms (minus the identity, for example), which cause the existence of so-called twists.

Explicitly ($N = 1$): let a, b and $d > 0$ in $\mathbb{Q}$ with d not a square, and with $4a^3 + 27b^2 \neq 0$, then $y^2 = x^3 + ax + b$ and $dy^2 = x^3 + ax + b$ define elliptic curves over $\mathbb{Q}$ that are not isomorphic over $\mathbb{Q}$, but become isomorphic after base change to $\mathbb{Q}(\sqrt{d})$. If X would be a fine moduli space for F_1, then the map $X(\mathbb{Q}) \to X(\mathbb{Q}(\sqrt{d}))$ would not be injective, while this map is injective for any scheme. This argument also shows that the morphism $j: F_1 \to \mathbb{A}^1_{\mathbb{Z}}$ that sends E/S to $j(E/S)$ in $\mathcal{O}_S(S) = \mathrm{Hom}_{\mathrm{Sch}}(S, \mathbb{A}^1_{\mathbb{Z}})$ is not an isomorphism. But still it is this kind of map that we want to generalize to arbitrary N. One can prove that this morphism j is universal for all morphisms from F_1 to schemes, which means, by the following definition, that $\mathbb{A}^1_{\mathbb{Z}}$ is a coarse moduli space for F_1.

4.2.1 Definition. *Let S be a scheme, $F: \mathrm{Sch}/S \to \mathrm{Set}$ a contravariant functor, and $\Phi: F \to h_X$ a morphism of functors. Then (X, Φ) is called a coarse moduli space for F if:*

1. *for every S-scheme $\mathrm{Spec}(k)$ with k an algebraically closed field, $\Phi(k): F(k) \to X(k)$ is bijective, and*

2. *for every S-scheme Y and every morphism $\Psi: F \to h_Y$, there exists a unique morphism $f: X \to Y$ such that $\Psi = h(f) \circ \Phi$.*

We remark that if such a pair (X, Φ) exists, then it is unique up to unique isomorphism by the second property. Recall that Yoneda's lemma says that $h: \mathrm{Hom}(X, Y) \to \mathrm{Hom}(h_X, h_Y)$ is bijctive, hence to demand, in the second property, a morphism from X to Y, or from h_X to h_Y, is equivalent. Note that if Φ is an isomorphism, then X is a fine moduli scheme for F.

4.2.2 Theorem. (Igusa) *Let $N \geq 1$. Then there exists a coarse moduli scheme $Y_0(N)_{\mathbb{Z}[1/N]}$ for F_N. The $\mathbb{Z}[1/N]$-scheme $Y_0(N)_{\mathbb{Z}[1/N]}$ is an affine smooth curve, with geometrically irreducible fibres. The natural bijection between $Y_0(N)_{\mathbb{Z}[1/N]}(\mathbb{C})$ and $\mathbb{H}/\Gamma_0(N)$ is an isomorphism of complex algebraic curves.*

The fact that $Y_0(N)_{\mathbb{Z}[1/N]}$ is a coarse moduli scheme for F_N implies that every pair $(E/S, G)$, with S a $\mathbb{Z}[1/N]$-scheme, E/S an elliptic curve and G a $\Gamma_0(N)$ structure on E/S, gives a morphism $S \to Y_0(N)_{\mathbb{Z}[1/N]}$, such that, for k an algebraically closed field, two k-valued points of S have the same image if and only if they define isomorphic elliptic curves with $\Gamma_0(N)$-structures over k. Furthermore, the universal property of coarse moduli spaces implies that every construction, that associates, functorially, to pairs $(E/A, G)$ an element of A, arises from a regular function on $Y_0(N)_{\mathbb{Z}[1/N]}$. For example, this defines the j-map from $Y_0(N)_{\mathbb{Z}[1/N]}$ to $\mathbb{A}^1_{\mathbb{Z}}$.

4.3 Description of Igusa's proof.

The proof of Igusa's theorem starts with the construction, completely by hand, of two fine moduli schemes that have to do with points of order 2 and 3 (Igusa actually used 3 and 4; we follow Katz and Mazur, and correct a mistake they make on page 112).

Let us consider the Legendre elliptic curve $\mathbb{E}/\mathbb{S}$ with $\mathbb{S} = \mathrm{Spec}(\mathbb{Z}[\lambda, (2\lambda(\lambda-1))^{-1}])$ and $\mathbb{E}$ given by the equation $y^2 = x(x-1)(x-\lambda)$. Let $P := (0,0)$, $Q := (1,0)$ and $\omega := (-dx)/2y$. Then $\Omega^1_{\mathbb{E}/\mathbb{S}} = \mathcal{O}_{\mathbb{E}}\omega$, $2P = 2Q = 0$, and 0, P and Q are disjoint. We put $t := 0^*\omega$ in $I(0)/I(0)^2$. Then t is a parameter at 0, up to first order, with $x^{-1} = t^2$ in $I(0)^2/I(0)^3$, and $y^{-1} = t^3$ in $I(0)^3/I(0)^4$.

Now suppose that A is a $\mathbb{Z}[1/2]$-algebra, that E/A is an elliptic curve, that P and Q are elements of $E(S)$ with $2P = 2Q = 0$ and with 0, P and Q disjoint, and that ω is a generator of $\Omega^1_{E/\mathbb{S}}$. We put $t := 0^*\omega$. Then, by a generalization of the argument that was done over fields in Mestre's lectures, E is given by a unique Weierstrass equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$, with $x^{-1} = t^2$ in $I(0)^2/I(0)^3$, $y^{-1} = t^3$ in $I(0)^3/I(0)^4$, and $x(P) = 0$. The facts that 0, P, Q and $P+Q$ are distinct, and that $2P = 2Q = 0$, imply that $x^3 + a_2x^2 + a_4x + a_6 = x(x - x(Q))(x - x(P+Q))$. Now we say that ω is adapted to P and Q if moreover $x(Q) = 1$, and we define a Legendre structure on E/A to be the data of P, Q and ω with P, Q in $E(A)$ with $2P = 2Q = 0$ and 0, P and Q disjoint, and ω a generator of $\Omega^1_{E/A}$ that is adapted to P and Q. Note that P, Q and ω as above define a Legendre structure on $\mathbb{E}/\mathbb{S}$. Suppose now that ω on E is adapted to P and Q. Then $(E/A, P, Q, \omega)$ is obtained from $(\mathbb{E}/\mathbb{S}, P, Q, \omega)$ in a unique way, i.e., there exists a unique morphism from $\mathrm{Spec}(A)$ to $\mathbb{S}$, and a unique isomorphism from E to the pullback of $\mathbb{E}$ to $\mathrm{Spec}(A)$, such that the data P, Q and ω on $\mathbb{E}$ are transformed into those on E. This implies that $\mathbb{S}$ is a fine moduli space for the contravariant functor $L\colon \mathrm{Sch}/\mathbb{Z}[1/2] \to \mathrm{Set}$, that sends S to the set of isomorphism classes of elliptic curves over S with a Legendre structure.

4.3.1 Remark. Note that the above property of the Legendre curve with its Legendre structure is actually a bit stronger than what we need: in addition to having a unique morphism from T to $\mathbb{S}$, we even get a unique isomorphism from E to the pullback of $\mathbb{E}$. This property can be conveniently phrased by saying that $(\mathbb{E}/\mathbb{S}, P, Q, \omega)$ is a final object in the category whose objects are $(E/S, P, Q, \omega)$ as above, and whose morphisms are cartesian diagrams:

$$\begin{array}{ccc} E & \to & E' \\ \downarrow & & \downarrow \\ S & \to & S' \end{array}$$

that are compatible with the Legendre structures on both sides. (Recall that such a diagram is called cartesian if it is a fibred product.) Such categories are called stacks in the book by Katz and Mazur, and in the article by Deligne and Rapoport. $\square$

On page 112 of the book by Katz and Mazur it is claimed that he universal property of $(\mathbb{E}/\mathbb{S}, P, Q, \omega)$ above gives an action by the group $\mathrm{GL}_2(\mathbb{F}_2) \times \{\pm 1\}$ on $\mathbb{E}/\mathbb{S}$: for g in this group there is unique diagram:

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{\alpha(g)} & \mathbb{E} \\ \downarrow & & \downarrow \\ \mathbb{S} & \xrightarrow{\beta(g)} & \mathbb{S} \end{array}$$

that transforms $((P, Q), \omega)g$ on the left to (P, Q, ω) on the right. The problem with this is that ω is not necessarily adapted to for example $(P, P+Q)$. A simple computation shows in fact that for all $g \neq 1$ in $\mathrm{GL}_2(\mathbb{F}_2)$ there does not exist a diagram as above, simply because $\beta(g)^*\mathbb{E}$ is a non-trivial twist of $\mathbb{E}$. In order to deal with this problem, we introduce the notion of a complete Legendre structure. For E/S an elliptic curve over a $\mathbb{Z}[1/2]$-algebra, a complete Legendre structure is a pair (ϕ, ω), with $\phi\colon (\mathbb{F}_2)_S^2 \to E[2]$ an isomorphism of S-group schemes, and $\omega \mathrm{GL}_2(\mathbb{F}_2) \to \Omega^1_{E/S}(E)$ a map such that for all g in $\mathrm{GL}_2(\mathbb{F}_2)$ the differential $\omega(g)$ is adapted to $\phi \circ g$ in the sense that it is adapted to $(\phi \circ g\binom{1}{0}, \phi \circ g\binom{0}{1})$.

Let G be the semi-direct product of $\mathrm{GL}_2(\mathbb{F}_2)$ by $\{\pm 1\}^{\mathrm{GL}_2(\mathbb{F}_2)}$ defined by the action of $\mathrm{GL}_2(\mathbb{F}_2)$ on itself by right-translations. For ε in $\{\pm 1\}^{\mathrm{GL}_2(\mathbb{F}_2)}$ and g in $\mathrm{GL}_2(\mathbb{F}_2)$, let (ε, g) denote the corresponding element in G, and define, for $(E/S, \phi, \omega)$ an elliptic curve with a complete Legendre structure:

$$(E/S, \phi, \omega) \cdot (\varepsilon, g) := (E/S, \phi \circ g, \varepsilon \cdot \omega \circ g),$$

where $\varepsilon \cdot \omega \circ g$ sends h to $\varepsilon(h)\omega(gh)$ (note that $\varepsilon(h)\omega(gh)$ is indeed adapted to $\phi \circ gh$).

A basic example of a complete Legendre structure is the following:

$$\mathbb{T}_0 = \mathrm{Spec}(\mathbb{Z}[1/2, \lambda, (\lambda(\lambda-1))^{-1}, i, \sqrt{\lambda}, \sqrt{\lambda - 1}]),$$

$$\mathbb{E} \text{ is given by } y^2 = x(x-1)(x-\lambda),\ \phi\tbinom{1}{0} = (0,0) \text{ and } \phi\tbinom{0}{1} = (1,0),$$

and

$$\begin{array}{rcl} \omega\colon\ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) & \mapsto & \omega_1 := (dx)/2y \\ \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) & \mapsto & \sqrt{\lambda}\,\omega_1 \\ \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right) & \mapsto & i\omega_1 \\ \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right) & \mapsto & \sqrt{\lambda-1}\,\omega_1 \\ \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) & \mapsto & i\sqrt{\lambda}\,\omega_1 \\ \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right) & \mapsto & i\sqrt{\lambda-1}\,\omega_1. \end{array}$$

If $(E/S/\mathbb{Z}[1/2], \phi, \omega)$ is a complete Legendre structure, then $(E/S/\mathbb{Z}[1/2], \phi, \omega(\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)))$ is obtained from $(\mathbb{E}/\mathbb{S}, P, Q, \omega)$ in a unique way. Moreover, we get square roots $\sqrt{\lambda}$, $\sqrt{-1}$, and $\sqrt{\lambda-1}$ on S from: $\omega(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)) = \sqrt{\lambda}\omega(1)$, $\omega(\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)) = \sqrt{\lambda}\omega(1)$ and $\omega(\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)) = \sqrt{\lambda}\omega(1)$. This gives a unique morphism from S to $\mathbb{T}_0$ which is compatible with the $\omega(g)$ for g different from $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$. So we get a universal elliptic curve with a complete Legendre structure $(\mathbb{E}/\mathbb{T}, \phi, \omega)$ by taking $\mathbb{T}$ a disjoint union of four copies of $\mathbb{T}_0$, over which $\mathbb{E}$ and ϕ are as above, and ω is changed by all possible combinations of signs at $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$.

By construction, we have an action by G on $\mathbb{E}/\mathbb{T}$: for g in G there is a unique diagram:

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{\alpha(g)} & \mathbb{E} \\ \downarrow & & \downarrow \\ \mathbb{T} & \xrightarrow{\beta(g)} & \mathbb{T} \end{array}$$

that transforms $(\phi\circ g, \varepsilon\omega\circ g)$ on the left to (ϕ, ω) on the right.

We can now quickly construct the restriction of $Y_0(N)_{\mathbb{Z}[1/N]}$ to $\mathbb{Z}[1/2N]$. Let $\mathbb{T}$ from now on denote $\mathbb{T}_{\mathbb{Z}[1/2N]}$, and $\mathbb{E}$ its restriction to the new $\mathbb{T}$. For each M dividing N, $\mathbb{E}[M]$ is a closed subscheme of $\mathbb{E}[N]$, but since both are finite etale over $\mathbb{T}$, it is also open (in fact, it is enough to note that $0(\mathbb{T})$ in $\mathbb{E}[N/M]$ is open, and that follows from the finite etaleness of $\mathbb{E}[N/M]$ over $\mathbb{T}$). So let X be the complement in $\mathbb{E}[N]$ of the union of the $\mathbb{E}[M]$ with M dividing N and $M \neq M$. Then X is the fine moduli space for elliptic curves over a $\mathbb{Z}[1/2N]$-scheme with a complete Legendre level structure, and a point P that has order N in every fibre. On X we have an action of the group $G' := G \times (\mathbb{Z}/N\mathbb{Z})^*$. We let $Y_0(N)_{\mathbb{Z}[1/2N]}$ be the quotient X/G'. It is then actually not so hard to show that this gives us a coarse moduli space over $\mathbb{Z}[1/2N]$ for the functor F_N defined above (restricted to $\mathbb{Z}[1/2N]$-schemes, of course).

A word about quotients. If a finite group G acts on a scheme X, then we define X/G to be the quotient in the category of locally ringed spaces. It is a good exercise to show that for X affine, say $\mathrm{Spec}(A)$, one has $X/G = \mathrm{Spec}(A^G)$, with A^G denoting the subring of G-invariants of A. It then follows that, in the general case, X/G is a scheme if every G-orbit is contained in an open affine. In the situation above, X is an affine curve, hence the quotient is a scheme. The fact that X is smooth implies the same for the quotient.

In the same way, and without extra effort, one can construct $Y_1(N)_{\mathbb{Z}[1/2N]}$ and $Y(N)_{\mathbb{Z}[1/2N]}$, which are even fine moduli spaces for $N \geq 4$ and $N \geq 3$, respectively.

Actually, it turns out that it is much simpler to work with trivializations of the full 4-torsion instead of the two-torsion and differential forms. Namely, it is very easy to construct by hand a universal elliptic curve with a point of order four, over $\mathbb{Z}[1/2]$-schemes. Here is the construction. Suppose that E is an elliptic curve over a $\mathbb{Z}[1/2]$-scheme S, and that P in $E(S)$ has order four in all fibres. Locally on S, choose arbitrary Weierstrass equations for E/S. These equations are unique up to the usual u, r, s and t. Now use r to get that $x(P)=0$; this is possible, and in a unique way of course, because $x(P)$ is a regular function (note that in all fibres $P\neq 0$). There exists a unique rational function f on E, of the form $x^2+\alpha y+\beta x+\gamma$, with divisor $4(P)-4(0)$. The element α is a unit, because, in all fibres, the divisor $4(P)-4(0)$ is not symmetric. Now use s and t in order to get $\beta=\gamma=0$; there are unique s and t to get that. Finally use u to get $\alpha=-1$; the required u is unique. By construction, substituting $y=x^2$ in the Weierstrass equation must give the equation $x^4=0$. This implies that there is a unique a such that E and P are given by:

$$E\colon y^2+xy+ay=x^3+ax^2, \quad P=(0,0).$$

A simple computation shows that $\Delta=a^4(1-16a)$. Our construction shows that the elliptic curve E given by the equation above, over the scheme:

$$Y_1(4)_{\mathbb{Z}[1/2]}=\mathrm{Spec}(\mathbb{Z}[1/2,a,(a(1-16a))^{-1}])$$

with its point $P:=(0,0)$, is universal. From this it is a simple matter to construct $Y(4)_{\mathbb{Z}[1/2]}$, the base of the universal curve with a full level four structure, i.e., with a trivialization of $E[4]$. One takes the open and closed subscheme of $E[4]$ on which the universal point Q gives, together with the point P, gives a $\mathbb{Z}/4\mathbb{Z}$-basis of $E[4]$. By construction, the group $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ acts on $E/Y(4)_{[\mathbb{Z}[1/2]}$.

What we have done up to now, using complete Legendre structures, or full level four structures over $\mathbb{Z}[1/2]$, can be imitated over $\mathbb{Z}[1/3]$ with full level three structures, which are, for E an elliptic curve over a $\mathbb{Z}[1/3]$-scheme, nothing but isomorphisms from $(\mathbb{Z}/3\mathbb{Z})^2_S$ to $E[3]$. The group G is then replaced by $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. The universal elliptic curve is in this case given by the equation $x^3+y^3+z^3-3\mu xyz$, over the ring $\mathbb{Z}[1/3,\zeta_3,\mu,(\mu^3-1)^{-1}]$. For other formulas see the book by Katz and Mazur.

So then we have our coarse moduli space for F_N both over $\mathbb{Z}[1/2N]$ and over $\mathbb{Z}[1/3N]$. The universal property gives an isomorphism between the two restrictions over $\mathbb{Z}[1/6N]$, by which one can glue them. The result of this glueing is then a coarse moduli space for F_N over $\mathbb{Z}[1/N]$.

Let $Y_0(N)_{\mathbb{C}}$ denote the pullback of $Y_0(N)_{\mathbb{Z}[1/N]}$ to $\mathbb{C}$. By construction, the set $Y_0(N)(\mathbb{C})$ of its $\mathbb{C}$-valued points is the set of isomorphism classes of elliptic curves with a cyclic subgroup of order N, which gives a bijection with $\mathbb{H}/\Gamma_0(N)$. Let us sketch a proof that this bijection is an isomorphism of Riemann surfaces. Let X be as above, in the construction of $Y_0(N)_{\mathbb{Z}[1/2N]}$. Over X we have the elliptic curve $\mathbb{E}$ with a complete Legendre structure, and a point that has order N everywhere. Extending scalars to $\mathbb{C}$, and passing to analytic varieties, we get similar analytic objects over $X(\mathbb{C})$. Let x be in $X(\mathbb{C})$. For U a small enough neighborhood of x, $0^*\Omega^1_{\mathbb{E}/X}$ is trivial on U, say generated by some ω, and the restriction of $\mathbb{E}(\mathbb{C})$ to U is homeomorphic to $S^1\times S^1\times U$ as a topological space over U (in fact there is an isomorphism of real analytic Lie groups over U; use that all the $\mathbb{E}[n]$ are finite etale, hence trivial over U). Integrating ω, in the fibres, over the two standard 1-cycles of $S^1 \times S^1$ shows that $\mathbb{E}(\mathbb{C})|_U$ arises from pullback from the elliptic curve over $\mathbb{H}$ whose fibre at τ is $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, in a compatible way with the extra structures we have on both sides. The universal property of the quotient map from $X(\mathbb{C})$ to $Y_0(N)(\mathbb{C})$ shows that the map from $Y_0(N)(\mathbb{C})$ to $\mathbb{H}/\Gamma_0(N)$ is analytic at the image of x.

4.4 Compactification of $Y_0(N)_{\mathbb{Z}[1/N]}$.

We have seen that the $Y_0(N)_{\mathbb{Z}[1/N]}$ are affine. We will construct a projective smooth $X_0(N)_{\mathbb{Z}[1/N]}$ that contains $Y_0(N)_{\mathbb{Z}[1/N]}$ as an open subscheme, whose complement is finite etale over $\mathbb{Z}[1/N]$. The method we use is completely analogous to the one we used to compactify $\mathbb{H}/\Gamma_0(N)$.

We have the morphism j from $Y_0(N)_{\mathbb{Z}[1/N]}$ to $\mathbb{P}^1_{\mathbb{Z}}$. We simply define $X_0(N)_{\mathbb{Z}}$ to be the normalization of $\mathbb{P}^1_{\mathbb{Z}}$ in the function field of $Y_0(N)_{\mathbb{Z}[1/N]}$. Concretely, this means that $X_0(N)_{\mathbb{Z}}$ is finite over $\mathbb{P}^1_{\mathbb{Z}}$, and that the inverse image of an affine open $\mathrm{Spec}(A)$ of $\mathbb{P}^1_{\mathbb{Z}}$ is $\mathrm{Spec}(B)$, for B the integral closure, also called the normalization, of A in the function field of $Y_0(N)_{\mathbb{Z}[1/N]}$ (such a construction does indeed "glue" because normalization commutes with localization). Since $Y_0(N)_{\mathbb{Z}[1/N]}$ is regular, and finite over $\mathbb{A}^1_{\mathbb{Z}[1/N]}$, it is the inverse image of $\mathbb{A}^1_{\mathbb{Z}[1/N]}$ in $X_0(N)_{\mathbb{Z}}$.

To study what happens "at ∞" we use Abhyankar's lemma (see SGA 1, XIII for general statements), which is an algebraic and higher dimensional version of the classification of unramified covers of the punctured disk that we considered when compactifying $Y_0(N)(\mathbb{C})$. In order to apply Abhyankar's lemma, we note that the j-morphism $Y_0(N)_{\mathbb{Z}[1/N]} \to \mathbb{A}^1_{\mathbb{Z}[1/N]}$ is finite etale over the complement of the closed subscheme defined by $j(j-1728)$, hence over a neighborhood around ∞ in $\mathbb{A}^1_{\mathbb{Z}[1/N]}$. Abhyankar's lemma then tells us that every point x in $\infty(\mathrm{Spec}(\mathbb{Z}))$ has an open neighborhood U, and a finite etale cover $\mathrm{Spec}(A) = U' \to U$, such that the A-scheme X', that is obtained from $X_0(N)_{\mathbb{Z}} \to \mathbb{P}^1_{\mathbb{Z}}$ by pullback to U', is a disjoint union of A-schemes of the form $\mathrm{Spec}(A[t]/(t^n - j^{-1}))$, with n dividing N.

It follows from this local description that $X_0(N)_{\mathbb{Z}}$ is smooth over $\mathbb{Z}[1/N]$, and that its reduced closed subscheme $\mathrm{Cusps}(X_0(N)_{\mathbb{Z}}) := X_0(N)_{\mathbb{Z}} - Y_0(N)_{\mathbb{Z}}$ is finite etale over $\mathbb{Z}[1/N]$. By construction, $X_0(N)_{\mathbb{Z}}$ is finite over $\mathbb{P}^1_{\mathbb{Z}}$, hence projective over $\mathbb{Z}$.

5 Hecke action on the $J_0(N)_{\mathbb{Z}[1/N]}$.

5.1 Atkin-Lehner involutions.

Let r and N be positive integers, with r dividing N and with r and N/r relatively prime. Suppose that $(E/S, G)$ is an elliptic curve with a $\Gamma_0(N)$-structure (with S necessarily a $\mathbb{Z}[1/N]$-scheme). Then we get an elliptic curve with a $\Gamma_0(N)$-structure, $(E/G, E[N]/G)$, where E/G is the quotient of E by its closed finite etale subgroup scheme G (locally finite etale on S the quotient can be constructed as the quotient by a the action of a finite group, and one performs a descent to get it on S itself; of course, I am not going to provide all the details here). This construction is a morphism w_r of functors from F_N to itself, and, in fact, an involution. By the universal property of coarse moduli schemes, induces an involution w_r of $Y_0(N)_{\mathbb{Z}[1/N]}$. We will now argue that this morphism extends, uniquely of course, to an involution w_r of $X_0(N)_{\mathbb{Z}[1/N]}$.

Let $X := X_0(N)_{\mathbb{Z}[1/N]}$, and let Z be the closure in $X \times X$ of the graph of w_r on $Y := Y_0(N)_{\mathbb{Z}[1/N]}$. Since w_r extends to an involution of $X_{\mathbb{Q}}$, just because $X_{\mathbb{Q}}$ is a proper and smooth curve, the two projections from Z to X are isomorphisms over certain cofinite open subsets of X. It follows that the two projections from Z to X are quasi finite, hence finite (here we use the properness of X over $\mathbb{Z}[1/N]$). Finally, since X is normal, both projections from Z to X are isomorphisms.

5.2 Degeneration morphisms.

Let N, M and d be positive integers with dM dividing N. Suppose that $(E/S, G)$ is an elliptic curve with a $\Gamma_0(N)$-structure. Then we get an elliptic curve with a $\Gamma_0(M)$-structure, $(E/G[d], \overline{G}[M])$, where $E/G[d]$ is the quotient of E by its closed finite etale subgroup scheme $G[d]$, and where $\overline{G}$ is the image of G in $E/G[d]$. This construction is a morphism of functors from F_N to F_M, hence, by the universal property of coarse moduli schemes, induces a morphism $B_d \colon Y_0(N)_{\mathbb{Z}[1/N]} \to Y_0(M)_{\mathbb{Z}[1/N]}$. We will now argue that this morphism extends, uniquely of course, to a morphism $B_d \colon X_0(N)_{\mathbb{Z}[1/N]} \to X_0(M)_{\mathbb{Z}[1/N]}$. For $d = 1$ this follows directly from the construction. For general d, the morphism $j \circ B_d$ from $Y_0(N)_{\mathbb{Z}[1/N]}$ to $\mathbb{A}^1_{\mathbb{Z}[1/N]}$ is equal to $j \circ w_d \circ B_1$, where B_1 goes from $Y_0(N)_{\mathbb{Z}[1/N]}$ to $Y_0(d)_{\mathbb{Z}[1/N]}$, w_d from $Y_0(d)_{\mathbb{Z}[1/N]}$ to itself, and j from $Y_0(d)_{\mathbb{Z}[1/N]}$ to $\mathbb{A}^1_{\mathbb{Z}[1/N]}$. We already know that these last three morphisms extend to the compactifications, so we know that $j \circ B_d$ extends to a morphism from $X_0(N)_{\mathbb{Z}[1/N]}$ to $\mathbb{P}^1_{\mathbb{Z}[1/N]}$. Both morphisms j and $j \circ B_d$ from $X_0(N)_{\mathbb{Z}[1/N]}$ and $X_0(M)_{\mathbb{Z}[1/N]}$ to $\mathbb{P}^1_{\mathbb{Z}[1/N]}$ are finite. It follows that the morphism B_d from $Y_0(N)_{\mathbb{Z}[1/N]}$ to $Y_0(M)_{\mathbb{Z}[1/N]}$ extends to a finite morphism from $X_0(N)_{\mathbb{Z}[1/N]}$ to $X_0(M)_{\mathbb{Z}[1/N]}$.

5.3 Hecke correspondences.

Let N be a positive integer, and p a prime number. As we have just seen that the degeneration morphisms extend to our compactifications, we have the Hecke correspondence:

$$
\begin{array}{ccc}
 & X_0(pN)_{\mathbb{Z}[1/pN]} & \\
{}^{B_p}\swarrow & & \searrow^{B_1} \\
X_0(N)_{\mathbb{Z}[1/pN]} & & X_0(N)_{\mathbb{Z}[1/pN]}
\end{array}
$$

5.4 The jacobian $J_0(N)_{\mathbb{Z}[1/N]}$.

To start, we want to have a $\mathbb{Z}[1/N]$-valued point of $X_0(N)_{\mathbb{Z}[1/N]}$. We have seen before that the set of cusps of $X_0(N)(\mathbb{C})$ is naturally isomorphic to $\left(\begin{smallmatrix}1&0\\ *&1\end{smallmatrix}\right)\backslash\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, with ∞ and 0 corresponding to $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, respectively. We have also seen that the ramification index of a cusp is the cardinality of the orbit that it corresponds to. Then it follows that 0 is the only cusp with ramification index N, hence it is $\mathbb{Q}$-rational. Since $\infty = w_N(0)$, the cusp ∞ is also $\mathbb{Q}$-rational. The fact that $X_0(N)_{\mathbb{Z}}$ is projective over $\mathbb{Z}$ implies that ∞ in $X_0(N)_{\mathbb{Z}}(\mathbb{Q})$ extends uniquely to an element ∞ in $X_0(N)_{\mathbb{Z}}(\mathbb{Z})$. As explained in the talks by Schoof, the contravariant functor from $\mathbb{Z}[1/N]$-schemes to the category of abelian groups given by $S \mapsto \mathrm{Pic}^0(X_0(N)_S)/\mathrm{Pic}(S)$ is represented by an abelian scheme that we will denote $J_0(N)_{\mathbb{Z}[1/N]}$.

We will now see how the morphisms in the previous sections give morphisms between these jacobians. Let us start with the Atkin-Lehner involutions. So let N and r be positive integers, with r dividing N, and such that r and N/r are relatively prime. Then we have the isomorphism w_r of $X_0(N)_{\mathbb{Z}[1/N]}$. We let it act, for every $\mathbb{Z}[1/N]$-scheme S, on $J_0(N)_{\mathbb{Z}[1/N]}(S)$, by the rule $\mathcal{L} \mapsto w_{r*}\mathcal{L}$. Since this is functorial in S, it defines an automorphism w_r of $J_0(N)_{\mathbb{Z}[1/N]}$.

Let us now consider degeneracy morphisms. So let N, M and d be positive integers with dM dividing N. Then, for every $\mathbb{Z}[1/N]$-scheme S, we have a map B_d^* from $J_0(M)_{\mathbb{Z}[1/N]}(S)$ to $J_0(N)_{\mathbb{Z}[1/N]}(S)$ given by $\mathcal{L} \mapsto B_d^*\mathcal{L}$. Likewise, we want to define a morphism B_{d*} in the other direction, as a kind of trace or norm map. In order to do that, it is good to note that the morphism B_d from $X_0(N)_{\mathbb{Z}[1/N]}$ to $X_0(M)_{\mathbb{Z}[1/N]}$ is finite and locally free. We have already seen that it is finite; the fact that it is locally free follows from the general result in commutative algebra that says that for A a noetherian regular local ring, every local regular A-algebra that is finite over A and of the same dimension as A is free as A-module. A reference for this result can be found in the book by Katz and Mazur, where the result is used many times.

So suppose that $f\colon X \to Y$ is a finite locally free morphism of schemes. Then the $\mathcal{O}_Y$-algebra $f_*\mathcal{O}_X$ is locally free as $\mathcal{O}_Y$-module, so that we have a norm map $f_*\mathcal{O}_X^* \to \mathcal{O}_Y^*$. We get a map f_* from $\mathrm{Pic}(X)$ to $\mathrm{Pic}(Y)$ as follows:

$$\mathrm{Pic}(X) = \mathrm{H}^1(X, \mathcal{O}_X^*) = \mathrm{H}^1(Y, f_*\mathcal{O}_X^*) \to \mathrm{H}^1(Y, \mathcal{O}_Y^*) = \mathrm{Pic}(Y),$$

where the second equality can be found somewhere in EGA II (one just needs to know that every invertible $\mathcal{O}_X$-module is trivial on open neighborhoods of the fibres of f, which is in fact a simple consequence of the Chinese remainder theorem).

Let us go back to our degeneracy morphism B_d. For every $\mathbb{Z}[1/N]$-scheme S, we have B_{d*} from $\mathrm{Pic}(X_0(N)_S)$ to $\mathrm{Pic}(X_0(M)_S$. This gives a morphism B_{d*} from $J_0(N)_{\mathbb{Z}[1/N]}$ to $J_0(M)_{\mathbb{Z}[1/N]}$. One easily verifies that $B_{d*}{\circ}B_d^*$ is multiplication by the degree of B_d on $J_0(M)_{\mathbb{Z}[1/N]}$.

Having these degeneracy morphisms act on jacobians by both Picard and Albanese functoriality, it is now a simple thing to define the action of Hecke correspondences. So let N be a positive integer, and p a prime number. We define T_p to be the endomorphism $B_{1*}{\circ}B_p^*$ of $J_0(N)_{\mathbb{Z}[1/pN]}$, and we define the T_n in $\mathrm{End}(J_0(N)_{\mathbb{Q}})$ for all $n \geq 1$ to be the endomorphisms given in terms of the T_p as in the second talk.

Let us remark that it is actually possible to extend the correspondences T_p over $\mathbb{Z}[1/N]$, at least if p does not divide N, and have the T_n act on $J_0(N)_{\mathbb{Z}[1/N]}$.

5.5 The cotangent space $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$.

Let $i\colon X_0(N)_{\mathbb{Q}} \to J_0(N)_{\mathbb{Q}}$ be the embedding that is normalized by $i(\infty) = 0$. Pullback of global one-forms then gives an isomorphism from $\Omega^1(J_0(N)_{\mathbb{Q}})$ to $\Omega^1(X_0(N)_{\mathbb{Q}})$. Since global one-forms on an abelian variety are translation invariant, evaluation at zero gives an isomorphism from $\Omega^1(J_0(N)_{\mathbb{Q}})$ to $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$. So, combined, this gives us an isomorphism from $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$ to $\Omega^1(X_0(N)_{\mathbb{Q}})$. On both these $\mathbb{Q}$-vector spaces we have defined endomorphisms T_n for all $n \geq 1$ (actually, the definition on $\Omega^1(X_0(N)_{\mathbb{Q}})$ has not been given, but we take the definition we have over $\mathbb{C}$ and replace $\mathbb{C}$ by $\mathbb{Q}$ in it). We want to know that the isomorphism just mentioned is compatible with the T_n, and with the B_d and the w_r. In order to do this, we recall some results about curves and their jacobians.

So suppose that X and Y are smooth projective geometrically irreducible curves over a field k, with given points x in $X(k)$ and y in $Y(k)$. Then we have the embeddings $i_x\colon X \to J_X$ and $i_y\colon Y \to J_Y$ of X and Y into their jacobians, that send a point P in X or Y to the class of the divisor $(P) - (x)$ or $(P) - (y)$. Suppose moreover that $f\colon X \to Y$ is a finite morphism. This gives us the following maps on cotangent spaces:

$$f_*\colon J_X \to J_Y \text{ induces } (f_*)^*\colon \mathrm{Cot}_0(J_Y) \to \mathrm{Cot}_0(J_X),$$

and

$$f^*\colon J_Y \to J_X \text{ induces } (f^*)^*\colon \mathrm{Cot}_0(J_X) \to \mathrm{Cot}_0(J_Y).$$

We claim that, under the isomorphisms above, $(f_*)^*$ is compatible with the map $f^*\Omega^1(Y) \to \Omega^1(X)$, and that $(f^*)^*$ is compatible with $f_*\colon \Omega^1(X) \to \Omega^1(Y)$. The first assertion follows directly from cconsideration of pullback of global one-forms in the commutative diagram:

$$\begin{array}{ccc} X & \to & J_X \\ \downarrow & & \downarrow \\ Y & \to & J_Y \end{array}$$

in which the horizontal maps are i_x and i_y, and the vertical maps f and f_*. The second assertion seems somewhat harder to prove. A consideration of line bundles on $X_{k[\varepsilon]}$ ($\varepsilon^2 = 0$) whose restriction to X is trivial, gives an isomorphism from $\mathrm{H}^1(X\mathcal{O}_X)$ to $\mathrm{Tan}_0(J_X)$. Since we have already an isomorphism from $\mathrm{Cot}_0(J_X)$ to $\Omega^1(X)$, we get a perfect pairing between $\Omega^1(X)$ and $\mathrm{H}^1(X\mathcal{O}_X)$. This pairing is, up to a sign that depends on various conventions, Serre duality. For Serre duality it is known that f_* and f^* are adjoint to each other (note that the possible sign does not matter, because in the compatibility it occurs twice). (However, it is a good exercise to make all definitions explicit, and to determine the sign. If I were to do it, I would start with an elliptic curve.)

So we know now that T_n on $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$ is compatible with T_n on $\Omega^1(X_0(N)_{\mathbb{Q}})$. We have an isomorphism:

$$\mathbb{C} \otimes \Omega^1(X_0(N)_{\mathbb{Q}}) = \Omega^1(X_0(N)_{\mathbb{C}}) \to S_2(\Gamma_0(N))_{\mathbb{C}},$$

which is compatible with T_n everywhere. This means that we can use the results from Frey's lectures on the action of the T_n on $S_2(\Gamma_0(N))_{\mathbb{C}}$ in order to study the action on $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$.

5.6 Decomposition of $J_0(N)_{\mathbb{Q}}$.

Let N be a positive integer. We let $\mathbb{T}$ (or $\mathbb{T}(N)$ if N needs to be specified) be the subring of $\mathrm{End}(J_0(N)_{\mathbb{Q}})$ that is generated by all T_n, $n \geq 1$. We let $\mathbb{T}'$ be the subring of $\mathbb{T}$ generated by the T_n with n prime to N. Since the endomorphism ring of an abelian variety is free of finite rank as a $\mathbb{Z}$-module, $\mathbb{T}$ and $\mathbb{T}'$ are both free $\mathbb{Z}$-modules of finite rank. The action of $\mathbb{T}$ on $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$ is faithful ($\mathbb{Q}$ has characteristic zero), hence we can view $\mathbb{T}_{\mathbb{C}} := \mathbb{C} \otimes \mathbb{T}$ as the sub-$\mathbb{C}$-algebra of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma_0(N))_{\mathbb{C}})$ generated by the T_n. Since the T_n with n relatively prime to N are self-adjoint for the Petersson scalar product, $\mathbb{T}'_{\mathbb{C}}$ is isomorphic to a product of copies of $\mathbb{C}$. But then $\mathbb{T}'_{\mathbb{Q}}$, being a commutative $\mathbb{Q}$-algebra of finite dimension, must be isomorphic to a product of fields, say $K_1 \times \cdots K_s$, with each K_i a finite extension of $\mathbb{Q}$. Moreover, $\mathbb{T}'$ itself is a subring of finite index in the product of the maximal orders of the K_i.

For $M \geq 1$, let $S_2(\Gamma_0(M))_{\mathbb{C}}^{\mathrm{new}}$ be the subspace of newforms in $S_2(\Gamma_0(M))_{\mathbb{C}}$; it is the intersection of the kernels of the B_{d*} for all d and M' with dM' dividing M and $M' \neq M$. This motivates us to define a quotient $J_0(M)_{\mathbb{Q},\mathrm{new}}$ of $J_0(N)_{\mathbb{Q}}$ by:

$$\bigoplus_{\substack{dM'|M \\ M'\neq M}} J_0(M')_{\mathbb{Q}} \xrightarrow{\Sigma B_d^*} J_0(M)_{\mathbb{Q}} \longrightarrow J_0(M)_{\mathbb{Q},\mathrm{new}} \longrightarrow 0.$$

By construction, $\mathrm{Cot}_0(J_0(M)_{\mathbb{C},\mathrm{new}})$ is then $S_2(\Gamma_0(M))_{\mathbb{C}}^{\mathrm{new}}$. The Atkin-Lehner theory of newforms tells us that the morphism:

$$J_0(N)_{\mathbb{Q}} \xrightarrow{\oplus B_{d*}} \bigoplus_{dM|N} J_0(M)_{\mathbb{Q},\mathrm{new}}$$

is an isogeny. Anyway, $\mathbb{T}'$ acts on $J_0(N)_{\mathbb{Q},\mathrm{new}}$, say with image of finite index in the maximal order of $K_1 \times \cdots \times K_t$. Each factor K_i of $K_1 \times \cdots \times K_t$ defines an isogeny factor A_i of $J_0(N)_{\mathbb{Q},\mathrm{new}}$. The multiplicity one result for the action of $\mathbb{T}'_{\mathbb{C}}$ on $S_2(\Gamma_0(N))_{\mathbb{C}}$ implies that each A_i has dimension $[K_i : \mathbb{Q}]$. We have an isogeny:

$$J_0(N)_{\mathbb{Q},\mathrm{new}} \to A_1 \times \cdots \times A_t.$$

The theorem of Kolyvagin and Logachev says that $A_i(\mathbb{Q})$ is finite if there exists an embedding of K_i into $\mathbb{C}$ such that the unique normalized newform $f = \sum a_n q^n$ with a_p equal to the image of T_p in $\mathbb{C}$ for all p not dividing N satisfies $L(f,1) \neq 0$. Of course, this theorem is a big step in proving the Birch-Swinnerton-Dyer conjecture for the abelian varieties $J_0(N)_{\mathbb{Q}}$.

6 Tangent spaces.

Let N be a positive integer, and p a prime not dividing N. Let $S := \mathrm{Spec}(\mathbb{Z}[1/N])$, $X := X_0(N)_S$ and $J := J_0(N)_S$. Let π denote the morphism from X to S. We have already seen that π is projective and smooth, and that the cusp ∞ in $X(\mathbb{C})$ defines an S-valued point ∞ in $X(S)$. Using Abhyankar's lemma, we have seen that $\mathrm{Cusps}(X) := (\jmath^{-1}\infty)_{\mathrm{red}}$ is finite and etale over S. It then follows that $\mathrm{Cusps}(X)$ is the disjoint union of $\infty(S)$ and another open and closed subscheme. It follows that, in a neighborhood of $\infty(S)$, j^{-1} is generator of the ideal of $\infty(S)$.

Let ∞_p be ∞ composed with the morphism $\mathrm{Spec}(\mathbb{F}_p) \to S$. Then ∞_p is in $X(\mathbb{F}_p)$, and $\mathcal{O}_{X,\infty_p}$ is a regular local ring in which (p, j^{-1}) is a system of parameters. Let X_p be the fibre of X over $\mathbb{F}_p$. Then the completion $\mathcal{O}^{\wedge}_{X_p,\infty_p}$ of $\mathcal{O}_{X_p,\infty_p}$ with respect to the maximal ideal is canonically isomorphic to $\mathbb{F}_p[[j^{-1}]]$, and cahence to $\mathbb{F}_p[[q]]$, where q and j are related in the usual way ($j = 1/q + 744 + \cdots$). Let $\mathrm{Cot}_{\infty_p}(X_p)$ denote the cotangent space of X_p at ∞_p; this is a one-dimensional $\mathbb{F}_p$-vector space, with basis dq. Let ∂ in $\mathrm{Tan}_{\infty_p}(X_p)$ be the basis dual to dq. Then ∂ is the derivation on $\mathbb{F}_p[[q]]$ that sends $\sum a_n q^n$ to a_1, the derivative at zero. By construction, $\partial(\sum_{n\geq 1} a_n q^n \, dq/q) = a_1$. This gives us a good understanding of the tangent space of X_p at ∞_p. Our next objctive is to do the same for $\mathrm{Cot}_0(J_p)$. As always for a smooth projective geometrically connected curve and its jacobian, we have:

$$\mathrm{Cot}_0(J_p) = \Omega^1(X_p).$$

6.1 Proposition. *$X_{\overline{\mathbb{F}}_p}$ is connected, and hence irreducible because non-singular.*

Proof. Grothendieck's theorem on formal functions (see Hartshorne, III, 11.1) says that the map:

$$W \otimes \mathcal{O}_X(X) = \mathcal{O}_{X_W}(X_W) \to \lim_n \mathcal{O}_{X_{W_n}}(X_{W_n}),$$

where W is the rinng of Witt vectors of $\overline{\mathbb{F}}_p$, and $W_n = W/p^nW$, is an isomorphism of W-algebras. Let K be the fraction field of W. Then $W \otimes \mathcal{O}_X(X)$ is a subring of $K \otimes \mathcal{O}_X(X) = \mathcal{O}_{X_K}(X_K)$, which is equal to K since $X_{\mathbb{C}}$, and hence X_K, are irreducible. Hence 0 and 1 are the only idempotents in the inverse limit of the $\mathcal{O}_{X_{W_n}}(X_{W_n})$, which means precisely that $X_{\overline{\mathbb{F}}_p}$ is connected. $\square$

6.2 Proposition. *The genus of $X_{\mathbb{C}}$ is equal to that of X_p.*

Proof. Since X_p is smooth, projective, and geometrically connected, we have $\mathcal{O}_{X_p}(X_p) = \mathbb{F}_p$. Since $X \to S$ is projective and smooth (hence flat), the Euler characteristic of $\mathcal{O}_X$ on the fibres is a constant function on S (see Hartshorne, III, 9.9). Hence the dimension of the $\mathbb{F}_p$-vector space $\mathrm{H}^1(X_p\mathcal{O}_{X_p})$ is that of the $\mathbb{C}$-vector space $\mathrm{H}^1(X_{\mathbb{C}}\mathcal{O}_{X_{\mathbb{C}}})$. Serre duality shows that $\Omega^1(X_p)$ and $\Omega^1(X_{\mathbb{C}})$ have the same dimension. $\square$

6.3 Proposition. *We have $\Omega^1(X_p) = \mathbb{F}_p \otimes \Omega^1(X)$.*

Proof. We consider the map $\Omega^1(X) \to \Omega^1(X_p)$, and we note that $\Omega^1_{X/S}$ is an invertible $\mathcal{O}_X$-module. On X we have the short exact sequence of $\mathcal{O}_X$-modules:

$$0 \longrightarrow \mathcal{O}_X \xrightarrow{p} \mathcal{O}_X \longrightarrow \mathcal{O}_{X_p} \longrightarrow 0.$$

Since $\Omega^1_{X/S}$ is locally free, tensoring this exact sequence by it gives an exact sequence. Since the formation of $\Omega^1_{X/S}$ (for general X and S) commutes with base change on S, we have an exact sequence:

$$0 \longrightarrow \Omega^1_{X/S} \xrightarrow{p} \Omega^1_{X/S} \longrightarrow \Omega^1_{X_p/\mathbb{F}_p} \longrightarrow 0.$$

Passing to global sections shows that the map from $\mathbb{F}_p \otimes \Omega^1(X)$ to $\Omega^1(X_p)$ is injective. Since $\Omega^1(X)$ is a $\mathbb{Z}[1/N]$-submodule of finite type in $\Omega^1(X_\mathbb{Q})$, with the property that $\mathbb{Q} \otimes \Omega^1(X) = \Omega^1(X_\mathbb{Q})$, $\Omega^1(X)$ is a free $\mathbb{Z}[1/N]$-module. It follows that our injection of $\mathbb{F}_p$-vector spaces is an isomorphism, because both spaces are of the same dimension. $\square$

Let us recall the definition of $S_2(\Gamma_0(N))_R$, for R any subring of $\mathbb{C}$: it is the R-module of elements f in $S_2(\Gamma_0(N))_\mathbb{C}$ whose q-expansion has coeffients in R.

6.4 Proposition. *The two sub-$\mathbb{Q}$-vector spaces $\Omega^1(X_\mathbb{Q})$ and $S_2(\Gamma_0(N))_\mathbb{Q}$ of $S_2(\Gamma_0(N))_\mathbb{C}$ are equal.*

Proof. Of course, it follows directly from the definitions that the q-expansion map from $\Omega^1(X_\mathbb{Q})$ to $S_2(\Gamma_0(N))_\mathbb{C}$ has image in $S_2(\Gamma_0(N))_\mathbb{Q}$. So it remains to prove the other inclusion. So let $\sum a_n q^n$ be in $S_2(\Gamma_0(N))_\mathbb{Q}$, and let $\omega = \sum a_n q^n \, dq/q$ in $\Omega^1(X_\mathbb{C})$ be its associated one-form. The fact that $\Omega^1(X_\mathbb{C}) = \mathbb{C} \otimes \Omega^1(X_\mathbb{Q})$ implies that $\sum a_n q^n$ is actually in the subring $\mathbb{C} \otimes \mathbb{Q}[[q]]$ of $\mathbb{C}[[q]]$. Let us consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \to & \Omega^1(X_\mathbb{Q}) & \to & \mathbb{C} \otimes \Omega^1(X_\mathbb{Q}) & \to & (\mathbb{C}/\mathbb{Q}) \otimes \Omega^1(X_\mathbb{Q}) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathbb{Q}[[q]] & \to & \mathbb{C} \otimes \mathbb{Q}[[q]] & \to & (\mathbb{C}/\mathbb{Q}) \otimes \mathbb{Q}[[q]] & \to & 0
\end{array}$$

The three vertical arrows are injective, simply because the functor $(\mathbb{C}/\mathbb{Q}) \otimes -$ is exact. The statement is now obvious. $\square$

6.5 Proposition. *The two $\mathbb{Z}[1/N]$-submodules $\Omega^1(X)$ and $S_2(\Gamma_0(N))_{\mathbb{Z}[1/N]}$ of $S_2(\Gamma_0(N))_\mathbb{C}$ are equal.*

Proof. As in the previous proof, the inclusion $\Omega^1(X) \subset S_2(\Gamma_0(N))_{\mathbb{Z}[1/N]}$ is clear. So let us suppose that $\sum a_n q^n$ is in $S_2(\Gamma_0(N))_{\mathbb{Z}[1/N]}$, and let ω be the corresponding element in $\Omega^1(X_\mathbb{Q})$. This means that ω is a rational section of the invertible $\mathcal{O}_X$-module $\Omega^1_{X/S}$. Since X is projective and smooth over S, it has all the properties one needs to work with divisors of rational sections of invertible $\mathcal{O}_X$-modules. In particular, the notions of Weil divisors and Cartier divisors are equivalent. The prime divisors of X are the following: the closures of the closed points of $X_0(N)_\mathbb{Q}$, and the irreducible components of the fibres over closed points of S. But since we know that all fibres are irreducible, the prime divisors of the last type are principal divisors:

X_p is the divisor of the funftion p. Let D be the divisor of ω. The fact that ω has no poles on $X_\mathbb{Q}$ means that all prime divisors of the first type have a multiplicity ≥ 0. Let p be a prime number, and consider the point ∞_p as before. We claim that the multiplicity D_p of X_p in D is exactly the minimum m_p of the $v_p(a_n)$, where v_p is the p-adic valuation on $\mathbb{Q}$, normalized by $v_p(p) = 1$. Obviously, m_p and D_p behave the same when one replaces ω by $p\omega$. Hence, in order to verify the claim, we may suppose that both D_p and m_p are ≥ 0. Recall that the completion of $\mathcal{O}_{X,\infty_p}$ with respect to its maximal ideal is $\mathbb{Z}_p[[q]]$. Now, the ideal in $\mathbb{Z}_p[[q]]$ defined by ω is the ideal generated by p^{m_p}, and also the ideal generated by p^{D_p}. It follows that m_p and D_p are equal. It is now clear that the divisor of the ω we started with is effective, hence that ω is in $\Omega^1(X)$. □

Combining the results above, we have:

$$\mathbb{F}_p \otimes S_2(\Gamma_0(N))_{\mathbb{Z}[1/N]} = \Omega^1(X_p) = \mathrm{Cot}_0(J_p) \to \mathrm{Cot}_{\infty_p}(X_p).$$

In the dual of $\mathrm{Cot}_{\infty_p}(X_p)$ we have our element ∂, inducing $\sum a_n q^n \mapsto a_1$ on $\mathbb{F}_p \otimes S_2(\Gamma_0(N))_{\mathbb{Z}[1/N]}$. We will also denote by ∂ the element $i_{\infty_p *}\partial$ of $\mathrm{Tan}_0(J_p)$, and we will write $\mathbb{T}_p$ for $\mathbb{F}_p \otimes \mathbb{T}$.

6.6 Theorem. *The tangent space* $\mathrm{Tan}_0(J_p)$ *is a free* $\mathbb{T}_p$*-module, with basis* ∂.

Proof. The statement is equivalent to saying that the pairing:

$$\mathrm{Cot}_0(J_p) \times \mathbb{T}_p \to \mathbb{F}_p, \quad (\omega, t) \mapsto a_1(t\omega),$$

is perfect. Note that both sides are $\mathbb{F}_p$-vector spaces of the same dimension (the genus of $X_\mathbb{C}$). Suppose that ω in $\mathrm{Cot}_0(J_p)$ has the property that $a_1(t\omega) = 0$ for all t in $\mathbb{T}$. Then, for all $n \geq 0$, $a_n(\omega) = a_1(T_n\omega) = 0$, which implies that ω is zero. □

7 The structure of $X_0(N)_{\mathbb{Z}}$ along the cusps.

In this section we state some results on the completion of $X_0(N)_{\mathbb{Z}}$ along the cusps, without justifying the computations. So let $N \geq 1$ be an integer, let $X := X_0(N)_{\mathbb{Z}}$, and let $X^\wedge$ be the completion of X along $\mathrm{Cusps}(X)$. In other words, $X^\wedge$ is the fibered product:

$$X^\wedge = \mathrm{Spec}(\mathbb{Z}[[q]]) \times_{\mathbb{P}^1_{\mathbb{Z}}} X.$$

Let $\mathrm{Tate}(q)$ denote the Tate elliptic curve over $\mathbb{Z}((q))$, as defined in the talks by Mestre. It follows from the construction of the Tate curve that we have:

$$\mathrm{Tate}(q)[N](\overline{\mathbb{Q}((q))}) = \{\zeta_N^a q^{b/N} \mid a, b \in \mathbb{Z}/N\mathbb{Z}\},$$

where ζ_N is a root of unity of order N, and $q^{1/N}$ a formal N-th root of q. One sees that the N-torsion of $\mathrm{Tate}(q)$ is rational over the extension $\mathbb{Q}(\zeta_N)((q^{1/N}))$ of $\mathbb{Q}((q))$. Let G be the Galois group of this extension. Then G is the semi-direct product of $(\mathbb{Z}/N\mathbb{Z})^*$ by μ_N, with u in $(\mathbb{Z}/N\mathbb{Z})^*$ acting on μ_N by $z \mapsto z^u$. Let C_N denote the set of cyclic subgroups of order N of $\mathrm{Tate}(q)[N](\overline{\mathbb{Q}((q))})$. Then we have:

$$C_N = \{\zeta_N^a q^{b/N} \mid (a, b) \text{ in } (\mathbb{Z}/N\mathbb{Z})^2 \text{ of order } N\}/(\mathbb{Z}/N\mathbb{Z})^*.$$

Define $Y^\wedge$ by:

$$Y^\wedge := \mathrm{Spec}(\mathbb{Z}((q))) \times_{\mathbb{P}^1_{\mathbb{Z}}} X.$$

Some thinking shows that we have:

$$(Y^\wedge)_{\mathbb{Q}} = \coprod_{G \backslash C_N} \mathrm{Spec}\left((\mathbb{Q} \otimes \mathbb{Z}[\zeta_N]((q^{1/N})))^{G_{\overline{(a,b)}}} \right),$$

where $\overline{(a,b)}$ denotes an element of C_N, and $G_{\overline{(a,b)}}$ its stabilizer in G. This is quite useful, since it allows one to compute $X^\wedge$, via:

$$X^\wedge \text{ is the normalization of } \mathrm{Spec}(\mathbb{Z}[[q]]) \text{ in } (Y^\wedge)_{\mathbb{Q}}.$$

We note that the set C_N is identified with $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, simply by associating (a, b) to $\zeta_N^a q^{b/N}$. Hence we see that the set of cusps of $X_{\mathbb{Q}}$ is the set $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \backslash \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. We have already seen that the set of cusps of $X_{\mathbb{C}}$ is $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \backslash \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$; the difference between the two is of course the action of the Galois group $(\mathbb{Z}/N\mathbb{Z})^*$.

Suppose now that $N = p^n$, with p a prime number. We choose the following representatives for $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \backslash \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$: $(0, 1)$, $(1, p^i)$ for $1 \leq i \leq n$. One computes that $G_{\overline{0,1}}$ is the group $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$, which gives a copy of $\mathrm{Spec}(\mathbb{Z}[[q^{1/p^n}]])$ in $X^\wedge$. Over this part, the given cyclic subgroup of the Tate curve is generated by q^{1/p^n}, which, in the way we have set things up, corresponds to τ/p^n in $\mathbb{H}$, hence to the cusp zero.

Clearly, $G_{\overline{(1,0)}} = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. In the same way as above, this gives a copy of $\mathrm{Spec}(\mathbb{Z}[[q]])$ in $X^\wedge$, over which one has the subgroup generated by ζ_N of the Tate curve. Obviously, this is the completion of X along ∞.

Suppose now that $1 \leq i < n$, and let $j := n - i$. One computes that $G_{\overline{(1,p^i)}} = \left(\begin{smallmatrix} 1 & x \\ 0 & 1+p^i x + p^j y \end{smallmatrix}\right)$, with x and y ranging over $\mathbb{Z}/p^n\mathbb{Z}$. For $i \geq n/2$, this gives a copy of $\mathrm{Spec}(\mathbb{Z}[\zeta_{p^j}][[q]])$ in $X^\wedge$, over which one has the subgroup generated by $\zeta_{p^n} q^{1/p^i}$ of the Tate curve. In terms of $\mathbb{H}$, this corresponds to $1/p^n + \tau/p^i$. For $i \leq n/2$ one gets a copy of the normalization of $\mathrm{Spec}(\mathbb{Z}[[q]])$ in $\mathbb{Z}[\zeta_{p^i}]((\zeta_{p^j}^{-1} q^{1/p^{n-2i}}))$. One can compute this normalization explicitly (see an article by myself in the Annales de l'Institut Fourier), but we know, using the Atkin-Lehner involution, that as a scheme it will be isomorphic to $\mathrm{Spec}(\mathbb{Z}[\zeta_{p^i}][[q]])$ (but not as a $\mathbb{Z}[[q]]$-scheme).

8 Some results from commutative algebra.

The aim of this section is to prove some results that were used in the previous sections, such as Abhyankar's lemma, and the fact that finite morphisms between regular schemes that are everywhere of the same dimension are locally free, using only results that the author of these notes himself fully understands. We only give a complete proof of Abhyankar's lemma in the case of dimension two. For the fact that certain finite morphisms $f: X \to Y$ were finite and locally free, let us note that we only used this when X and Y were smooth projective curves over some base. The flatness then follows from the fibre-wise criterion for flatness (see EGA).

8.1 Theorem. *Let A be a local ring which is noetherian, normal, and of dimension at least two. Let B be the intersection, in the field of fractions K of A, of the localizations of A at its prime ideals of height one. Then $B = A$.*

Proof. Let $M \subset B$ be a finitely generated A-module containing A, and let $\overline{M} := M/A$. By induction on $\dim(A)$ we know that the support of $\overline{M}$ is contained in $\{m\}$, where m is the maximal ideal of A (localize at the non-maximal prime ideals of A). Hence $\overline{M}$ is annihilated by m^n for some $n \geq 0$. For each $i \geq 0$, let $N_i := \{a \in K \mid a{\cdot}m^n \subset A\}$. Then we have:

$$A = N_0 \subset N_1 \subset \cdots \subset N_n, \text{ and } M \subset N_n.$$

Consider N_1. We have either $N_1 m = A$ or $N_1 m = m$. Suppose that $N_1 m = A$. Then there exists n in N_1 and a in A such that $na = 1$. Krull's Hauptidealsatz gives us a prime ideal y of height one such that $v_y(a) > 0$ (v_y is the valuation associated to y), hence with $v_y(n) < 0$. Now take b in m, such that b is not in y; then $v_y(b) = 0$, and, because b is in m, nb is in A. This is a contradicion, because $v_y(nb) = v_y(n) + v_y(b) < 0$.

Hence we know that $N_1 m = m$. But then $N_1 N_1 m = N_1 m = m \subset A$, which implies that $N_1 N_1 \subset N_1$. So N_1 is an A-sub-algebra of K, which is finitely generated as A-module, hence equal to A because A is normal. Now note that $mN_i \subset N_{i-1}$, for $i \geq 1$, which gives $N_i = A$ for all $i \geq 1$. □

8.2 Theorem. *Let A be a local noetherian normal ring. Let $X := \mathrm{Spec}(A)$, let Y be a closed subset of X of codimension at least two, let $U := X - Y$ and let $j: U \to X$ be the inclusion. Finally, let $\mathcal{F}$ be a locally free $\mathcal{O}_U$-module of finite rank. Then $\mathcal{F}(U)$ is a finitely generated A-module, and $j_*\mathcal{F}$ is the coherent $\mathcal{O}_X$-module associated to it.*

Proof. We note first that $j_*\mathcal{F}$ is quasi-coherent, because j is quasi-compact and separated (note that the ideal of Y is finitely generated, and see Hartshorne, II, 5.8). It follows that $j_*\mathcal{F}$ is the quasi-coherent $\mathcal{O}_X$-module associated to the A-module $\mathcal{F}(U)$. It remains to show that $\mathcal{F}(U)$ is finitely generated. We first prove this for $\mathcal{O}_U$ itself. But, in the notation of the preceding theorem, $\mathcal{O}_U(U)$ is contained in B, hence equal to A. Let $\mathcal{F}^\vee$ denote the $\mathcal{O}_U$-linear dual of $\mathcal{F}$. If we can show that $\mathcal{F}^\vee$ is a quotient of $\mathcal{O}_U^n$ for some n, then $\mathcal{F}$ is a sub-$\mathcal{O}_U$-module of $\mathcal{O}_U^n$ for that n, which implies that $\mathcal{F}(U)$ is an A-submodule of A^n, hence finitely generated.

We claim that in fact any coherent $\mathcal{O}_U$-module $\mathcal{G}$ is a quotient of some $\mathcal{O}_U^n$. Here is the proof. First of all, $j_*\mathcal{G}$ is quasi-coherent by the same argument as above for $\mathcal{F}$; hence $j_*\mathcal{G}$ is the quasi-coherent $\mathcal{O}_X$-module associated to the A-module $N := \mathcal{G}(U)$. Let $x_1, \ldots, x_r$ be a system of generators for the ideal of Y. For $1 \leq i \leq r$ let $g_{i,j}$, $1 \leq j \leq n_i$, be a finite set of generators for the A_{x_i}-module N_{x_i}. After multiplying the $g_{i,j}$ by suitable powers of x_i, we may assume that the $g_{i,j}$ are in N. It is clear that the $g_{i,j}$ generate the $\mathcal{O}_U$-module $\mathcal{G}$. $\square$

8.3 Theorem. *Let A be a noetherian regular local ring of dimension two. Let $X := \operatorname{Spec}(A)$, x in X the closed point and $j: U = X - \{x\} \to X$ the inclusion. Let $\mathcal{F}$ be a locally free $\mathcal{O}_U$-module of finite rank. Then $j_*\mathcal{F}$ is a free $\mathcal{O}_X$-module of finite rank.*

Proof. According to the previous theorem, $j_*\mathcal{F}$ is the quasi-coherent $\mathcal{O}_X$-module associated to the finitely generated A-module $M := \mathcal{F}(U)$. Let k be the residue field of A. It remains to be shown that the dimension over k of $k \otimes_A M$ is (at most) the rank of $\mathcal{F}$. Let a, b be a system of generators of the maximal ideal of A. Let V be the closed subscheme of U defined by the equation $a = 0$, and let $i: V \to U$ denote the closed immersion. We have an exact sequence of $\mathcal{O}_U$-modules:

$$0 \longrightarrow \mathcal{O}_U \xrightarrow{a} \mathcal{O}_U \longrightarrow i_*\mathcal{O}_V \longrightarrow 0.$$

Since $\mathcal{F}$ is locally free, tensoring by it gives an exact sequence:

$$0 \longrightarrow \mathcal{F} \xrightarrow{a} \mathcal{F} \longrightarrow i_*i^*\mathcal{F} \longrightarrow 0.$$

Passing to sections over U gives an exact sequence:

$$0 \longrightarrow M \xrightarrow{a} M \longrightarrow (i^*\mathcal{F})(V),$$

which shows that M/aM is a sub-A/aA-module of $(i^*\mathcal{F})(V)$. Now note that A/aA is a discrete valuation ring with uniformizer b, and that $(i^*\mathcal{F})(V)$ is a vector space over its field of fractions of dimension the rank of $\mathcal{F}$. It follows that M/aM is torsion free as A/aA-module, hence free of rank at most the rank of $\mathcal{F}$. Hence $M/(aM + bM)$ is of dimension at most the rank of $\mathcal{F}$. $\square$

8.4 Remark. The condition that A is of dimension two, in the previous theorem, is really necessary. In fact, the only dimensions in which such a result is true are zero and two. For example, for k a field and $d \geq 3$, indecomposable vector bundles of rank at least two on $\mathbb{P}_k^{d-1}$ give counterexamples by pulling them back to $\mathbb{A}_k^d - \{0\} \subset \mathbb{A}_k^d$. $\square$

8.5 Theorem. *Let A be a noetherian strictly henselian regular local ring of dimension two (for example, $W[[t]]$, with W a complete discrete vauation ring with separably closed residue field). Let $X := \operatorname{Spec}(A)$, x the closed point of X, and U its complement. Let $f: U' \to U$ be finite etale, and let $X' \to X$ be the normalization of X in U'. Then $X' \to X$ is finite etale.*

Proof. Let $j: U \to X$ be the inclusion. Note that $f_* \mathcal{O}_{U'}$ is a locally free $\mathcal{O}_U$-module. By the previous theorem, $j_* f_* \mathcal{O}_{U'}$ is a locally free $\mathcal{O}_X$-module, with an $\mathcal{O}_X$-algebra structure. Put $B := j_* f_* \mathcal{O}_{U'}(X)$, and $X' := \mathrm{Spec}(B)$. Then $X' \to X$ extends $U' \to U$ as a finite free morphism. The ramification locus of this morphism is defined by one equation, the discriminant. But then this discriminant must be a unit, since otherwise f would be ramified at a point of codimension one, and those are in U. □

8.6 Remark. The theorem above is called the purity theorem of Nagata and Zariski, in dimension two. The result is actually true in all dimensions $d \geq 2$. For a proof see SGA 2, X, 3.4. The idea of the proof is to do induction on the dimension by passing to a closed subscheme of X of the form $V(t)$ with t a parameter of A. Then one compares the finite etale covers of U, X, $U^\wedge$, $X^\wedge$ and $V(t)$, where $U^\wedge$ and $X^\wedge$ are the completions of U and X along $V(t) \cap U$ and $V(t)$, respectively. □

In order to state Abhyankar's lemma, we need some terminology. Let X be a regular noetherian scheme, D a reduced effective divisor on X, and $U := X - D$. Let $U' \to U$ be finite etale, and let $X' \to X$ be the normalization of X in U'. Let η be the generic point of an irreducible component of D, and let η' be a point of X' that maps to η. Then U' is said to be tamely ramified at η' if the extension of discrete valuation rings $\mathcal{O}_{X,\eta} \to \mathcal{O}_{X',\eta'}$ is tamely ramified, i.e., if the residue field extension $k(\eta) \to k(\eta')$ is separable, and the ramification index invertible in $k(\eta)$. The cover U' of U is said to be tamely ramified over D if it is tamely ramified at all combinations (η, η'). Note that if all $k(\eta)$ are of characteristic zero, then every finite etale $U' \to U$ is tame.

8.7 Theorem. *Let A be a noetherian complete regular local ring with separably closed residue field. Let $t_1, \ldots, t_r$ be a set of parameters in A, i.e., the t_i are in the maximal ideal m of A, with linearly independent images in the $k := A/m$-vector space m/m^2. Let $D := V(t_1 \cdots t_r)$, $U := X - D$, and $U' \to U$ finite etale and tamely ramified over D. Let X' be the normalization of X in U'. Then, as an X-scheme, X' is isomorphic to a disjoint union of schemes of the form:*

$$\mathrm{Spec}(A[x_1, \ldots, x_r]/(x_1^{n_1} - t_1, \ldots, x_r^{n_r} - t_r))/G,$$

with the n_i invertible in A, and G a subgroup of $\mu_{n_1} \times \cdots \times \mu_{n_r}$. In particular, if $r = 1$, then X' is isomorphic to a disjoint union of copies of $A[x]/(x^n - t)$, with the n invertible in A.

Proof. First we do some reductions in the general case, and then finish the proof in the case of dimension at most two. A proof of the general case can be found in SGA 1, XIII, §5.

Let $S' \to S$ be a finite etale morphism, with S' connected and $S \to S'$ surjective. A construction that is analogous to the construction of a splitting field for a polynomial shows that $S' \to S$ is dominated by a finite etale cover $S'' \to S$ that is Galois over S in the following sense: one has a group G acting freely of S'', such that $S'' \to S$ is the quotient morphism. The morphism $S'' \to S'$ is then the quotient for some subgroup H of G. We apply this construction to a connected component of U', and get a U'', a G and an H as above. We claim that we can choose U'' to be tame over U. In fact, we claim that there is a maximal tame cover U^t between U'' and U. To construct it, let $N \subset G$ be the subgroup generated by the elements g of G that act trvially on some $\mathcal{O}_{X'',\eta''}/m_{\eta''}^2$, where X'' is the normalization of X in U'', η'' the generic point of an irreducible component of the inverse image D'' of D in X''. Then N is a normal subgroup of G, and $U^t := U/N$ has the desired properties. So, from now on, we assume that $U'' \to U$ is Galois, with group G, and tame, and that $U' = U''/H$.

Let n_i be the ramification index of U'' over U at the generic point of $D_i := V(t_i)$, and define:

$$Y := \mathrm{Spec}(A[x_1, \ldots, x_r]/(x_1^{n_1} - t_1, \ldots, x_r^{n_r} - t_r)),$$

and let Y'' be the normalization of Y in $Y \times_X U''$. Let V and V'' be the inverse images of U in Y and Y'', respectively. We claim that $Y'' \to Y$ is finite etale. This is so by construction over V, since $V \to U$ is finite etale. Once we know that Y'' is finite etale over Y at the generic points of the $V(x_i)$, we know it ove all of Y by the purity theorem above (that we have proved in the case of dimension two). So let η be the generic point of some $V(t_i)$, and η'' an element of the fibre of $X'' \to X$ over η. Let n be the ramification index at η''. Let $G_{\eta''}$ be the stabilizer in G of η'', and let $I_{\eta''}$ be the kernel for the action of $G_{\eta''}$ on $k(\eta'')$. Then $\mathcal{O}_{X,\eta}^\wedge$ is $(\mathcal{O}_{X'',\eta''}^\wedge)^{G_{\eta''}}$, the ring of $G_{\eta''}$-invariants in the completion of $\mathcal{O}_{X'',\eta''}$ with respect to its maximal ideal $m_{\eta''}$. The subgroup $I_{\eta''}$ acts on $m_{\eta''}/m_{\eta''}^2$ via an isomorphism $\chi\colon I_{\eta''} \to \mu_n(k(\eta''))$. Let π be a uniformizer of $\mathcal{O}_{X'',\eta''}$. After replacing π by $\sum_g \chi(g)^{-1} g\pi$, with g ranging over $I_{\eta''}$, we have $g\pi = \chi(g)\pi$ for all g in $I_{\eta''}$, i.e., we have linearized the action. It is then clear that $\pi^n = t_i u_i$, with u_i a unit in $(\mathcal{O}_{X'',\eta''}^\wedge)^{I_{\eta''}}$, which is unramified over $\mathcal{O}_{X,\eta}^\wedge$. For simplicity, let us put $B := \mathcal{O}_{X,\eta}^\wedge$, $C := \mathcal{O}_{X'',\eta''}^\wedge$ and $t := t_i$. Put $B' := B[x]/(x^n - t_i)$, and let C' be the normalization of $B' \otimes_B C$. Then C' is obtained from C by first doing an unramified extension C'', and then normalizing $C''[y]/(y^n - x^n u)$. It is easy to see that this is also unramified. This calculation finishes the proof that $Y'' \to Y$ is finite etale at the generic points of the $V(t_i)$.

Now we know that Y'' is finite etale over Y. But since Y is itself the spectrum of a noetherian complete regular local ring with separable closed residue field, Y'' is a disjoint union of copies of Y itself. This gives us a morphism from Y to X'', over X. Hence Y dominates the X' we were interested in. Now note that Y has an obvious action by the X-group scheme $G := \mu_{n_1} \times \cdots \times \mu_{n_r}$, which makes Y into a G-torsor over X. The fact that $Y \to X$ is tamely ramified implies that all n_i are invertible on X, for, if not, the action of some μ_{n_i} on $V(x_i)$ would cause a non-tivial inseparable sub-extension in the funtion fields of $V(t_i)$ and $V(x_i)$. (I am aware that more details would be welcome here.) Hence, in fact, the group scheme G is just constant, and the proof is finished. $\square$