Explicit adelic description of moduli of elliptic curves and Galois action on CM-points

Gabor Wiese

June 10, 2003

Abstract

These are notes of two talks in the local number theory seminar in Leiden on Shimura varieties given on 26 May and 2 June 2003.

The aim is to treat a very simple example of a Shimura variety, namely the moduli space of elliptic curves together with a certain limit of level structures, without entering into the entire formalism. In the first talk, we shall give several descriptions of this space and obtain a very natural action of the absolute Galois group on it. The second talk will introduce a very elegant language for dealing with the Galois action on elliptic curves with complex multiplications by a fixed quadratic imaginary field. We will formulate the main theorem of complex multiplications on elliptic curves, but won't prove it.

Both talks were explained to me by Bas Edixhoven. The principal contents can also be found in Deligne-Rapoport.

Contents

1 Elliptic curves with level structures

In this first part we will establish several bijections, providing us with different descriptions of the moduli space of elliptic curves with a full level n structure.

Elliptic curves over $\mathbb{C}$ and lattices

Let us, however, start without level structures. We denote by $\mathrm{Ell}(\mathbb{C})$ the category of elliptic curves $E(\mathbb{C})$ over $\mathbb{C}$, with isomorphisms as morphisms. We want to relate this to the category $\mathrm{Lat}(\mathbb{C})$ of lattices $\Lambda < \mathbb{C}$ with morphisms given by multiplication by a complex number.

There is a well-known equivalence of categories between $\mathrm{Lat}(\mathbb{C})$ and $\mathrm{Ell}(\mathbb{C})$ given by sending a lattice $\Lambda < \mathbb{C}$ to the Riemann surface $\mathbb{C}/\Lambda$. Recalling that, up to isomorphism, every elliptic curve over $\mathbb{C}$ is of that form, it follows that we have indeed an equivalence of categories. This implies that there is a bijection of sets

$$_{\cong}\backslash\mathrm{Lat}(\mathbb{C}) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad _{\cong}\backslash\mathrm{Ell}(\mathbb{C}).$$

Aside on homology

Since in the actual talk I used things like $H_1(E(\mathbb{C}), \mathbb{Z})$, I ought to say some words about that here.

If I understand it well, there really is no need for using this slightly fancy language. For, if we are working up to isomorphism, we can always take $H_1(E(\mathbb{C}), \mathbb{Z})$ to be the lattice Λ, and if it is up to isogeny, well, then we choose some lattice Λ and tensor it with $\mathbb{Q}$, over $\mathbb{Z}$. Having killed any motivation on this point, I will go on to explain it nevertheless.

We start by recalling the definition of $H_1(X, \mathbb{Z})$ for a real manifold X. A short one would be to say that it is the abelianisation of the fundamental group of X.

Very often, one finds simplicial homology. We do a very special case here. By a *path* we mean a continuous map $\phi : [0, 1] \to X$. Let $\mathbb{Z}$[paths] be the free abelian group generated by the paths. There is a natural boundary map ∂_1 given uniquely by sending a path ϕ to $\phi(1) - \phi(0)$, the end point minus the starting point in the free abelian group generated by the points. An element z in the kernel of ∂_1 is called a *cycle*. The set of cycles is denoted $Z_1(X, \mathbb{Z})$.

Let Δ_2 be the set of elements in $(x, y, z) \in \mathbb{R}^3_{\geq 0}$ such that $x + y + z = 1$. It is a description of a triangular surface. (If one notices that $(x, y) \in \mathbb{R}^2_{\geq 0}$ with $x + y = 1$ gives the line segment from $(1, 0)$ to $(0, 1)$, which is homeomorphic with $[0, 1]$, then it is evident, how to continue to higher dimensions.) A *face* is now a continuous map $\Phi : \Delta_2 \to X$. Also faces have boundaries. Namely

$\partial_2(\Phi)$ is the cycle that is naturally given by the obvious boudary of the triangular surface. The set of all boundaries of faces is denoted $B_1(X, \mathbb{Z})$.

The first homology $H_1(X, \mathbb{Z})$ is the quotient (of abelian groups) $Z_1(X, \mathbb{Z})/B_1(X, \mathbb{Z})$. Given an abelian group A, one can replace $\mathbb{Z}$ by A in the above definition to obtain $H_1(X, A)$.

An important theorem says that for a compact oriented complex curve X of genus g, the group $H_1(X, \mathbb{Z})$ is a free abelian group of rank $2g$, and that $H_1(X, A) = H_1(X, \mathbb{Z}) \otimes_{\mathbb{Z}} A$.

Let now an elliptic curve $E(\mathbb{C})$ be given as $\mathbb{C}/\Lambda$. It is clear that the universal covering space of $E(\mathbb{C})$ is $\mathbb{C}$ and that the fundamental group is abelian, and generated by any two paths that span the lattice. Thus we see that $H_1(E(\mathbb{C}), \mathbb{Z}) = \Lambda$. Consequently, $H_1(E(\mathbb{C}), \mathbb{R}) = \mathbb{C}$. So, we can now think of an elliptic curve $E(\mathbb{C})$ as the quotient $H_1(E(\mathbb{C}), \mathbb{R})/H_1(E(\mathbb{C}), \mathbb{Z})$.

If one wants to avoid using the description "$\mathbb{C}/\Lambda$" to obtain "1-dimensional $\mathbb{C}$-vector space modulo lattice", one has to use the Abel-Jacobi map. For this we recall that the space $\Omega^1(E(\mathbb{C}))$ of holomorphic differentials on a compact Riemann surface of genus g is a g-dimensional $\mathbb{C}$-vector space. Differentials can be integrated along paths. Let us embed $H_1(E(\mathbb{C}), \mathbb{Z})$ into $\Omega^1(E(\mathbb{C}))^\vee$, by sending a path α to the linear form $\omega \mapsto \int_\alpha \omega$. Now we can write down the Abel-Jacobi map.

$$E(\mathbb{C}) \to \Omega^1(E(\mathbb{C}))^\vee / H_1(E(\mathbb{C}), \mathbb{Z}), \quad P \mapsto (\omega \mapsto \int_0^P w).$$

It is now the theorem of Abel-Jacobi that this is an isomorphism. Thus we find the description $\mathbb{C}$ modulo lattice, used before.

Let us recall that the dual of the holomorphic diffentials is also called the tangent space (at 0): $\mathcal{T}_0(E(\mathbb{C}))$.

Torsion points and the Tate module

We denote by $E(\mathbb{C})[n]$ the kernel of the multiplication by n map on an elliptic curve $E(\mathbb{C})$:

$$0 \to E(\mathbb{C})[n] \to E(\mathbb{C}) \xrightarrow{\cdot n} E(\mathbb{C}) \to 0$$

for a non-zero integer n.

If $E(\mathbb{C}) = \mathbb{C}/\Lambda$, then one finds $E(\mathbb{C})[n] = \frac{1}{n}\Lambda/\Lambda$. The *Tate module* $T(E(\mathbb{C}))$ is defined as the projective limit over the $E(\mathbb{C})[n]$. Moreover, one (and we, too) uses a lot the $\mathbb{Q}$-vector space $V(E(\mathbb{C})) = T(E(\mathbb{C})) \otimes_{\mathbb{Z}} \mathbb{Q}$.

In the rather fancy language from above one has

$$E(\mathbb{C})[n] = H_1(E(\mathbb{C}), \mathbb{Z}/n), \quad T(E(\mathbb{C})) = H_1(E(\mathbb{C}), \hat{\mathbb{Z}}), \quad V(E(\mathbb{C})) = H_1(E(\mathbb{C}), \mathbb{A}_f).$$

Level structures and lattices

Now consider level structures. We introduce the category $\mathrm{Ell}^n(\mathbb{C})$ of *elliptic curves with a full level n structure*, whose objects are pairs $(E(\mathbb{C}), \phi^n)$ with $E(\mathbb{C})$ an elliptic curve and ϕ^n an isomorphism from $(\mathbb{Z}/n)^2$ to $E(\mathbb{C})[n]$. The morphisms are the isogenies (and the zero) respecting the ϕ^ns (in the sense one thinks, which I am too lazy to put into a commutative diagram right now).

We want to relate this category with lattices. Well, the obvious choice is the category $\mathrm{Lat}^n(\mathbb{C})$, with objects (Λ, ϕ^n). Here Λ is a lattice in $\mathbb{C}$, and ϕ^n is an isomorphism (of groups) between $(\mathbb{Z}/n)^2$ and $\frac{1}{n}\Lambda/\Lambda$. The morphisms are those $\mathbb{C}$-linear maps that respect the ϕ^ns.

In the same way as above, one obtains a bijection

$$_{\cong}\backslash \mathrm{Lat}^n(\mathbb{C}) \overset{\text{bij.}}{\longleftrightarrow} {}_{\cong}\backslash \mathrm{Ell}^n(\mathbb{C}).$$

Complex structures

Let V be a 2-dimensional real vector space. In Robert's talk complex structures on V were introduced as $\mathbb{R}$-algebra homomorphisms $\mathbb{C} \to \mathrm{End}_{\mathbb{R}}(V)$. I call the set of complex structures $\mathrm{CS}(V)$. Such an $\mathbb{R}$-algebra homomorphism ψ determines what multiplication by a complex number should be: multiplication by $z \in \mathbb{C}$ corresponds to application of the matrix $\psi(z)$.

Of course, it is enough to know what multiplication by i does. We have $\psi(i)^2 = \psi(i^2) = \psi(-1) = -1$. So $\psi(i)$ has two eigenvalues i and $-i$ (considering $\psi(i)$ to act on the complexified vector space $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$). The eigenspace of $V_{\mathbb{C}}$ corresponding to i is not stabilized by complex conjugation, as otherwise it would also be an eigenspace for $-i$. For any non-real 1-dimensional vector space W in $V_{\mathbb{C}}$, there is a $\psi(i)$ such that W is the i-eigenspace of $\psi(i)$. This yields a bijection between $\mathrm{CS}(V)$ and $\mathbb{P}(V_{\mathbb{C}}) \setminus \mathbb{P}(V)$.

We have a $\mathrm{GL}(V)$-action on $\mathrm{CS}(V)$ given by conjugation: $(M.\psi)(z) = M(\psi(z))M^{-1}$. On the eigenspace side, this corresponds to $M.W = MW$.

If we now identify $\mathbb{P}(V_{\mathbb{C}}) \setminus \mathbb{P}(V)$ with $\mathbb{C} \setminus \mathbb{R} = \mathbb{H}^{\pm}$, the action on the right space is by fractional linear transformations. Let us make the resulting bijection $\mathrm{CS}(V) \overset{\text{bij.}}{\longleftrightarrow} \mathbb{H}^{\pm}$ explicit. Given a complex structure $\psi : \mathbb{C} \to \mathrm{End}_{\mathbb{R}}(V)$, choose a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M^{-1}$ equals $\psi(i)$. The element of $\mathbb{H}^{\pm}$ we map to is $\frac{ai+b}{ci+d}$.

Real lattices

Let us introduce the category $\mathrm{Lat}^n(\mathbb{R}^2)$, whose objects are pairs (Λ, ϕ^n) with $\Lambda \leq \mathbb{R}^2$ a lattice and ϕ^n an isomorphism between $(\mathbb{Z}/n)^2$ and $\frac{1}{n}\Lambda/\Lambda$. The morphisms are elements of $\mathrm{GL}_2(\mathbb{R})$ respecting the ϕ^ns.

We have a natural bijection

$$_{\cong}\backslash(\mathrm{CS}(\mathbb{R}^2) \times \mathrm{Lat}^n(\mathbb{R}^2)) \quad \stackrel{\text{bij.}}{\longleftrightarrow} \quad _{\cong}\backslash\mathrm{Lat}^n(\mathbb{C})$$

because the isomorphisms on the left are required to respect the complex structure. Hence only those matrices in $\mathrm{GL}_2(\mathbb{R})$ are allowed that correspond to multiplication by elements of $\mathbb{C}^*$.

Let us remark that if we have any isomorphism between pairs (ψ_1, Λ_1) and (ψ_2, Λ_2) in $\mathrm{CS}(\mathbb{R}^2) \times \mathrm{Lat}^n(\mathbb{R}^2)$, then there is a matrix $M \in \mathrm{GL}_2(\mathbb{R})$ such that $\Lambda_2 = M\Lambda_1$ and $\psi_2 = M \circ \psi_1 \circ M^{-1}$. Consequently, the isomorphism classes are precisely the $\mathrm{GL}_2(\mathbb{R})$-orbits, yielding a bijection

$$\mathrm{GL}_2(\mathbb{R})\backslash(\mathrm{CS}(\mathbb{R}^2) \times \mathrm{Lat}^n(\mathbb{R}^2)) \quad \stackrel{\text{bij.}}{\longleftrightarrow} \quad _{\cong}\backslash\mathrm{Lat}^n(\mathbb{C})$$

Rational lattices

This is the point where the first trick comes. One reduces to structures that one has over $\mathbb{Q}$. Namely, we consider the category $\mathrm{Lat}^n(\mathbb{Q}^2)$, defined in the obvious way similarly to the others. In every $\mathrm{GL}_2(\mathbb{R})$-orbit of (Λ, ψ^n) with $\Lambda < \mathbb{R}_2$ there is an element $(M\Lambda, M \circ \psi^n)$ for some $M \in \mathrm{GL}_2(\mathbb{R})$ such that $M\Lambda < \mathbb{Q}^2 < \mathbb{R}^2$. This yields the bijection

$$\mathrm{GL}_2(\mathbb{R})\backslash(\mathrm{CS}(\mathbb{R}^2) \times \mathrm{Lat}^n(\mathbb{R}^2)) \quad \stackrel{\text{bij.}}{\longleftrightarrow} \quad \mathrm{GL}_2(\mathbb{Q})\backslash(\mathrm{CS}(\mathbb{R}^2) \times \mathrm{Lat}^n(\mathbb{Q}^2)).$$

Adelic lattices

The second trick is to consider $\hat{\mathbb{Z}}$-lattices in ${\mathbb{A}_f}^2$. So, let's denote by $\mathrm{Lat}({\mathbb{A}_f}^2)$ the category of $\hat{\mathbb{Z}}$-lattices, whose morphisms are given by $\mathrm{GL}_2(\mathbb{A}_f)$.

From Robert's talk we know that there is a bijection

$$\mathrm{Lat}(\mathbb{Q}^2) \quad \stackrel{\text{bij.}}{\longleftrightarrow} \quad \mathrm{Lat}({\mathbb{A}_f}^2),$$

given by $\Lambda < \mathbb{Q}^2 \mapsto \Lambda \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ and in the other direction by $L < {\mathbb{A}_f}^2 \mapsto L \cap \mathbb{Q}^2$.

Analogously to the preceding, we also consider the category $\mathrm{Lat}^n({\mathbb{A}_f}^2)$ of pairs (L, ϕ^n), now with $\phi^n : (\mathbb{Z}/n)^2 \to \frac{1}{n}L/L$. As one has that $\frac{1}{n}L/L = \frac{1}{n}\Lambda/\Lambda$, one obtains a bijection

$$\mathrm{Lat}^n(\mathbb{Q}^2) \quad \stackrel{\text{bij.}}{\longleftrightarrow} \quad \mathrm{Lat}^n({\mathbb{A}_f}^2).$$

We now relate the category $\mathrm{Lat}^n({\mathbb{A}_f}^2)$ to the group $\mathrm{GL}_2(\mathbb{A}_f)$. Let us first note that there is a natural bijection between the set of $\hat{\mathbb{Z}}$-lattices $L < {\mathbb{A}_f}^2$ together with an isomorphism $\psi : \hat{\mathbb{Z}}^2 \to L$, just by taking the lattice spanned by the two columns of the matrix. There is an obvious transitive action by $\mathrm{GL}_2(\mathbb{A}_f)$ on it. Now we define the group K_n for a natural number n by the exact sequence

$$0 \to K_n \to \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n) \to 0.$$

The pair $(\hat{\mathbb{Z}}^2, \phi^n)$ in $\mathrm{Lat}^n({\mathbb{A}_f}^2)$, with ϕ^n the identity, is precisely stabilized by K_n. Hence we obtain a bijection

$$\mathrm{Lat}^n({\mathbb{A}_f}^2) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad \mathrm{GL}_2(\mathbb{A}_f)/K_n.$$

Characterisation of the moduli space

We now recall from last year's geometry seminar that there is an affine scheme over $\mathbb{Q}$, denoted Y_{K_n} and called the *modular curve with full level n structure*, whose $\mathbb{C}$-points are precisely $_{\cong}\backslash\mathrm{Ell}^n(\mathbb{C})$. We ought to remark that Y_{K_n} is only a fine moduli space if $n \geq 3$.

Putting all the bijections just developped together one obtains

$$Y_{K_n}(\mathbb{C}) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad \mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)/K_n\big).$$

2 The associated Shimura variety Y

We define the *associated Shimura variety* Y as the projective limit over the affine $\mathbb{Q}$-schemes Y_{K_n}. Let us remark that if each of the Y_{K_n} is given as $\mathrm{Spec}(A_n)$ with a $\mathbb{Q}$-algebra A_n, then Y is the spectrum of the injective limit over the A_n. It is hence, as claimed, again a $\mathbb{Q}$-scheme, however, not of finite type.

We will again find natural interpretations of the complex points of this scheme as certain moduli of elliptic curves. Before being able to start that, we will look a bit closer at the structure of $\mathrm{GL}_2(\mathbb{A}_f)$.

Properties of $\mathrm{GL}_2(\mathbb{A}_f)$

Given a topological ring R, the group $\mathrm{GL}_2(R)$ carries the relative topology as a closed subset in R^5. It is the subset consisting of those (a, b, c, d, e) such that $e \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$.

Let us first apply this to the rings $\hat{\mathbb{Z}}$ and $\mathbb{Z}/n$, the latter with the discrete topology. Taking the projective limit over the embeddings $\mathrm{GL}_2(\mathbb{Z}/n) \hookrightarrow (\mathbb{Z}/n)^5$ we see that the topology on $\mathrm{GL}_2(\hat{\mathbb{Z}})$ as a profinite group equals the topology it carries as a subset of $\hat{\mathbb{Z}}^5$.

The only sensible topology on the group $\mathrm{GL}_2(\mathbb{A}_f)$ seems to be the topology as a subset of ${\mathbb{A}_f}^5$. With it, it is clear that $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is open in $\mathrm{GL}_2(\mathbb{A}_f)$, since $\hat{\mathbb{Z}}$ is open in $\mathbb{A}_f$.

Proposition 2.1 *The $K_n < \mathrm{GL}_2(\mathbb{A}_f)$ form a basis of open neighbourhoods of $1 \in \mathrm{GL}_2(\mathbb{A}_f)$.*

Proof. We use both topologies. The profinite one gives us that K_n is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ because it is the kernel (with a finite quotient) of a continuous homomorphism. Since the subset topology has yielded that $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is open in $\mathrm{GL}_2(\mathbb{A}_f)$, the K_n are also open in $\mathrm{GL}_2(\mathbb{A}_f)$. By definition of the profinite topology they form a basis of open neighbourhoods of $1 \in \mathrm{GL}_2(\hat{\mathbb{Z}})$, hence also of $\mathrm{GL}_2(\mathbb{A}_f)$. ☐

A first bijection

We know that we have the bijection $Y_{K_n}(\mathbb{C}) \overset{\text{bij.}}{\longleftrightarrow} \mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)/K_n\big)$.

There is the following proposition (a proof of which I will maybe add later).

Proposition 2.2 *Let $n \geq 3$. Then $\mathrm{GL}_2(\mathbb{Q})$ acts freely on $\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)/K_n$.*

Corollary 2.3 $\varprojlim_n \mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)/K_n\big) \cong \mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)\big)$.

Proof. By the topology of $\mathrm{GL}_2(\mathbb{A}_f)$ (discussed above), it is clear that $\varprojlim_n \mathrm{GL}_2(\mathbb{A}_f)/K_n$ equals $\mathrm{GL}_2(\mathbb{A}_f)$. Moreover, we have hence a natural surjection

$$\mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)\big) \to \varprojlim_n \mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)/K_n\big),$$

the injectivity of which is left to prove.

Let us regard projective limits as subsets of the direct product $\prod \mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)/K_n\big)$. Given any two $x, y \in \mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)$ mapping to the same element on the right, we have to show the existence of a $g \in \mathrm{GL}_2(\mathbb{Q})$ such that $gx = y$.

Write x_n, y_n for the images in $\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)/K_n$. By assumption for each n there is a $g_n \in \mathrm{GL}_2(\mathbb{Q})$ such that $g_n x_n = y_n$. Next we have to use the compatibility of the $\mathrm{GL}_2(\mathbb{Q})$-action with the transition maps. This implies directly that $g_{nm}x_n = g_n x_n$ for all natural numbers n, m. At this point we can use the proposition to conclude that $g_n = g_m = g_{nm}$, provided $n, m \geq 3$. This finishes the proof because we can choose our g to be g_3, which is equal to g_n for all $n \geq 3$, and take the projective limit only over those n greater equal 3 (not changing the limit). ☐

Consequently, we have a bijection

$$Y(\mathbb{C}) \overset{\text{bij.}}{\longleftrightarrow} \mathrm{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{A}_f)\big).$$

Elliptic curves up to isogeny

Let us first describe a construction that works for any additive category using the example $\mathrm{Ell}(\mathbb{C})$.

Define the category $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ to have as objects $E(\mathbb{C}) \otimes \mathbb{Q}$ (meant formally) with $E(\mathbb{C})$ an object of $\mathrm{Ell}(\mathbb{C})$. The morphisms are defined to be

$$\mathrm{Hom}_{\mathrm{Ell}(\mathbb{C})\otimes\mathbb{Q}}(E_1(\mathbb{C}) \otimes \mathbb{Q}, E_2(\mathbb{C}) \otimes \mathbb{Q}) = \mathrm{Hom}_{\mathrm{Ell}(\mathbb{C})}(E_1(\mathbb{C}), E_2(\mathbb{C})) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

(We see that all we use is that the morphisms form an abelian group and that composition is bilinear, which is one of the demands on an additive category.)

The title of this paragraph is justified by the following proposition.

Proposition 2.4 *Let $E_1(\mathbb{C}), E_2(\mathbb{C})$ be two elliptic curves. Then $E_1(\mathbb{C})$ and $E_2(\mathbb{C})$ are isogenous if and only if $E_1(\mathbb{C}) \otimes \mathbb{Q}$ and $E_2(\mathbb{C}) \otimes \mathbb{Q}$ are isomorphic.*

Proof. Let $\phi : E_1(\mathbb{C}) \to E_2(\mathbb{C})$ be an isogeny with kernel $K \subseteq E_1(\mathbb{C})[n]$. We then consider the composition

$$E_1(\mathbb{C}) \xrightarrow{\phi} E_2(\mathbb{C}) \xrightarrow{\psi} E_1(\mathbb{C})/K \xrightarrow{\cdot n} E_1(\mathbb{C}).$$

It is precisely multiplication by n on $E_1(\mathbb{C})$. We can write this as $(\psi \otimes n)(\phi \otimes 1) = \mathrm{id} \otimes n$, which is a unit. Hence, $\phi \otimes 1$ has a left inverse. The existence of a right inverse is also evident.

On the other hand, an isomorphism in $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ can be written as $\phi \otimes 1/n$ for some $\phi : E_1(\mathbb{C}) \to E_2(\mathbb{C})$. Say, it has left inverse $\psi \otimes 1/r$. Then $\psi \circ \phi \otimes 1 = \mathrm{id} \otimes nr$. Consequently, the kernel of ϕ is contained in $E_1(\mathbb{C})[nr]$, which makes ϕ an isogeny. $\square$

Earlier, we had a bijection $_{\cong}\backslash\mathrm{Ell}(\mathbb{C}) \overset{\text{bij.}}{\longleftrightarrow} {}_{\cong}\backslash\mathrm{Lat}(\mathbb{C})$. Now replacing $\mathrm{Ell}(\mathbb{C})$ by $\mathrm{Ell}(\mathbb{C})\otimes\mathbb{Q}$, we obtain a bijection

$$_{\cong}\backslash\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q} \overset{\text{bij.}}{\longleftrightarrow} {}_{\cong}\backslash\{V < \mathbb{C} \mid V \text{ a 2-dim. } \mathbb{Q}\text{-v.s. s.t. } V \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{C}\ \}.$$

Starting with an elliptic curve $\mathbb{C}/\Lambda$, we send it to $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$. Or in more fancy language $E(\mathbb{C}) \mapsto H_1(E(\mathbb{C}), \mathbb{Q})$. The reason why this works is that if we have two lattices $\Lambda_1, \Lambda_2 \in V$, then we always find an n such that $n\Lambda_1 \leq \Lambda_2 \leq \frac{1}{n}\Lambda_1$.

Also as above, we can go one step further, and obtain a bijection

$$_{\cong}\backslash\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q} \overset{\text{bij.}}{\longleftrightarrow} {}_{\cong}\backslash\{\ (V, \tau)\ \},$$

where V is a 2-dimensional $\mathbb{Q}$-vector space, and $\tau \in \mathrm{CS}(V_{\mathbb{R}})$ is a complex structure on $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$.

A second bijection

Let us continue in the spirit of the preceding paragraph. We introduce the category ShEll($\mathbb{C}$), whose objects are pairs $(E(\mathbb{C}) \otimes \mathbb{Q}, \psi)$ with $E(\mathbb{C}) \otimes \mathbb{Q} \in$ Ell($\mathbb{C}$) $\otimes\, \mathbb{Q}$ and ψ an isomorphism of $\mathbb{A}_f$-modules ${\mathbb{A}_f}^2 \to V(E(\mathbb{C}))$. We ought to mention at this point that the functor V from Ell($\mathbb{C}$) to $\mathbb{A}_f$-modules factors through Ell($\mathbb{C}$) $\otimes\, \mathbb{Q}$.

From the above, we immediately conclude that we have a bijection

$$_{\cong}\backslash\text{ShEll}(\mathbb{C}) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad _{\cong}\backslash\{\ (V, \tau, \psi)\ \},$$

with V a 2-dimensional $\mathbb{Q}$-vector space, $\tau \in \text{CS}(V_{\mathbb{R}})$ a complex structure on $V_{\mathbb{R}}$ and ψ an $\mathbb{A}_f$-isomorphism ${\mathbb{A}_f}^2 \to V \otimes_{\mathbb{Q}} \mathbb{A}_f$.

I should maybe point out that $V(E(\mathbb{C}) \otimes \mathbb{Q}) = V(E(\mathbb{C})) = H_1(E(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \hat{\mathbb{Z}}$. Hence, $V(E)$ only depends on the isogeny class of $E(\mathbb{C})$.

Instead of the V, let us now always take $\mathbb{Q}^2$. Then we have a bijection between $_{\cong}\backslash\{\ (V, \tau, \psi)\ \}$ and $_{\cong}\backslash\{\ (\tau, \psi)\ \}$, now with τ a complex structure on $\mathbb{Q}^2_{\mathbb{R}} = \mathbb{R}^2$ and ψ and isomorphism ${\mathbb{A}_f}^2 \to \mathbb{Q}^2 \otimes_{\mathbb{Q}} \mathbb{A}_f = {\mathbb{A}_f}^2$, i.e. $\psi \in \text{GL}_2(\mathbb{A}_f)$. The isomorphisms allowed are, however, only elements of $\text{GL}_2(\mathbb{Q})$. Consequently, we have a bijection

$$_{\cong}\backslash\{\ (V, \tau, \psi)\ \} \quad \overset{\text{bij.}}{\longleftrightarrow} \quad \text{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \text{GL}_2(\mathbb{A}_f)\big).$$

Characterisation of $Y(\mathbb{C})$

Putting the results together, we have bijections

$$Y(\mathbb{C}) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad \text{GL}_2(\mathbb{Q})\backslash\big(\mathbb{H}^{\pm} \times \text{GL}_2(\mathbb{A}_f)\big) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad _{\cong}\backslash\text{ShEll}(\mathbb{C}).$$

Without proof, I'd like to add that the above sets are also in bijection with

$$_{\cong}\backslash\{\ (E, \phi) \mid E \in \text{Ell}(\mathbb{C}),\ \phi : \hat{\mathbb{Z}}^2 \to T(E(\mathbb{C})) \text{ a } \hat{\mathbb{Z}}\text{-isom.}\ \}.$$

3 Actions on Y

We have two important group actions on the $\overline{\mathbb{Q}}$-points of Y. Clearly, $Y(\overline{\mathbb{Q}})$ is in bijection with $_{\cong}\backslash$ShEll($\overline{\mathbb{Q}}$), where ShEll($\overline{\mathbb{Q}}$) is the subcategory of ShEll($\mathbb{C}$) whose objects are those defined over $\overline{\mathbb{Q}}$.

Galois action

Let us recall that Y is a scheme over $\mathbb{Q}$. Consequently, one has an action by the absolute Galois group $G_{\mathbb{Q}} = G(\overline{\mathbb{Q}}|\mathbb{Q})$ on $Y(\overline{\mathbb{Q}})$.

Let $\sigma \in G_{\mathbb{Q}}$. Then one has a bijection $E(\overline{\mathbb{Q}}) \to \sigma E(\overline{\mathbb{Q}})$, given by applying σ to the points. This also gives us an isomorphism $V(E(\overline{\mathbb{Q}})) \to V(\sigma E(\overline{\mathbb{Q}}))$, denoted $V(\sigma)$.

It is clear what the Galois action on $Y(\overline{\mathbb{Q}})$ corresponds to on ShEll($\overline{\mathbb{Q}}$); namely, we send a pair $(E(\overline{\mathbb{Q}}), \psi)$ to $(\sigma E(\overline{\mathbb{Q}}), V(\sigma) \circ \psi)$.

$\mathrm{GL}_2(\mathbb{A}_f)$-action

On $Y(\overline{\mathbb{Q}})$ we also have a natural action by $\mathrm{GL}_2(\mathbb{A}_f)$. Given $g \in \mathrm{GL}_2(\mathbb{A}_f)$ and a pair (E, ψ) we define $(E, \psi).g$ to be $(E, \psi \circ g)$.

Since this action means composing ψ from the right and the Galois action composing from the left, the associativity of composition of maps yields that the two actions commute.

We would, however, like the $\mathrm{GL}_2(\mathbb{A}_f)$-action to be an action on the scheme Y. That is true, but does not seem to be completely obvious. One way to do it is the following. We have used that Y_{K_n} is an affine scheme over $\mathbb{Q}$. It is a theorem by Deligne, that for any compact open subgroup $K \in \mathrm{GL}_2(\mathbb{A}_f)$, one has a $\mathbb{Q}$-scheme Y_K. Then the limit $\varprojlim_n Y_{K_n}$ equals $\varprojlim_{K < \mathrm{GL}_2(\mathbb{A}_f) \text{ open compact}} Y_K$ because the Y_{K_n} form a cofinal system. Now given a $g \in \mathrm{GL}_2(\mathbb{A}_f)$, one has an isomorphism of $\mathbb{Q}$-schemes

$$Y_K \to Y_{gKg^{-1}}.$$

Passing to the projective limit, one obtains the desired automorphism of Y corresponding to the action of g.

In the appendix I treat a functorial point of view on Y, which is technically quite complicated. However, it also implies that the group $\mathrm{GL}_2(\mathbb{A}_f)$ acts on the scheme Y.

4 CM-theory

Elliptic curves with complex multiplication

Let F be an imaginary quadratic field, for which we choose, once and for all, an embedding $\iota : F \hookrightarrow \mathbb{C}$.

Let $E(\mathbb{C})$ be an elliptic curve over $\mathbb{C}$. One says that $E(\mathbb{C})$ has *complex multiplication by* F if the endomorphism ring $\mathrm{End}(E(\mathbb{C}))$ is an order of F. That is the case if and only if $\mathrm{End}(E(\mathbb{C})) \otimes_{\mathbb{Z}} \mathbb{Q} = F$.

One way to identify $\mathrm{End}(E(\mathbb{C}))$ with an order (as a subring of $\mathbb{C}$) is as follows. Take $\phi \in \mathrm{End}(E(\mathbb{C}))$, it acts as multiplication by a complex number z on $H_1(E(\mathbb{C}), \mathbb{Z}) < \mathbb{C}$. Send ϕ to z. This, moreover, yields a ring homomorphism $\mathrm{End}(E(\mathbb{C})) \otimes \mathbb{Q} \to \mathbb{C}$, which is well defined for an element of Ell$(\mathbb{C}) \otimes \mathbb{Q}$.

Let $\mathcal{O}_{F,c}$ be an order of F. We then have a bijection

$$\mathrm{CL}(\mathcal{O}_{F,c}) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad {}_{\cong}\backslash\{\ E(\mathbb{C}) \mid E(\mathbb{C}) \in \text{Ell}(\mathbb{C}) \text{ with } \mathrm{End}(E(\mathbb{C})) = \mathcal{O}_{F,c}\ \},$$

given by mapping an ideal $\mathfrak{a}$ to $\mathbb{C}/\mathfrak{a}$.

From this it follows that up to isogeny there is just one elliptic curve with complex multiplication by F.

Proposition 4.1 *In the isomorphism class of any elliptic curve $E(\mathbb{C}) \in$ Ell$(\mathbb{C})$ with complex multiplication, there is a representative that is already defined over $\overline{\mathbb{Q}}$.*

Proof. From the finiteness of class groups it follows that there are only finitely many isomorphism classes of elliptic curves with endomorphism ring equal to a given order in F. For any $\sigma \in \mathrm{Aut}(\mathbb{C}|\mathbb{Q})$ the rings $\mathrm{End}(E(\mathbb{C}))$ and $\mathrm{End}(\sigma(E(\mathbb{C})))$ are isomorphic. Hence the orbit of $j(E(\mathbb{C}))$ is finite. Consequently, $j(E(\mathbb{C}))$ cannot be transcendental. Thus in the isomorphism class there is an elliptic curve that is defined over $\overline{\mathbb{Q}}$. $\square$

Proposition 4.2 *For any elliptic curve $E(\mathbb{C})$ over the complex numbers with complex multiplication by the imaginary quadratic field F the $\mathbb{A}_{F,f}$-module $V(E(\mathbb{C}))$ is a free of rank 1.*

Proof. $\mathrm{End}(E(\mathbb{C}))$ acts by multiplication with an element of F on $H_1(E(\mathbb{C}), \mathbb{Q})$, as the discussion at the beginning of this paragraph shows. Hence, we have an action of F on $V(E(\mathbb{C})) = H_1(E(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{A}_f$, making the free $\mathbb{A}_f$-module of rank 2 into a free rank 1 $\mathbb{A}_{F,f}$-module. $\square$

Moduli of elliptic curves with CM by F

We consider the category ShEll$_F(\mathbb{C})$, whose objects are triples $(E(\mathbb{C}) \otimes \mathbb{Q}, \alpha, \psi)$. Here, $E(\mathbb{C}) \otimes \mathbb{Q}$ is in Ell$(\mathbb{C}) \otimes \mathbb{Q}$. The second component α is a ring homomorphism $F \to \mathrm{End}(E(\mathbb{C})) \otimes \mathbb{Q}$, on which we impose that it is, composed with the embedding $\mathrm{End}(E(\mathbb{C})) \otimes \mathbb{Q}$ into $\mathbb{C}$ described above, equal to ι. This serves to choose one of the two possible α. Finally, ψ is an isomorphism of $\mathbb{A}_{F,f}$-modules $\mathbb{A}_{F,f} \to V(E(\mathbb{C}))$. Thus the extra structure coming from CM is reflected. The morphisms are the obvious ones.

Let us denote ${}_{\cong}\backslash$ShEll$_F(\mathbb{C})$ by $S_F(\mathbb{C})$. From the discussion above we see (with the obvious definition for ShEll$_F(\overline{\mathbb{Q}})$) that $S_F(\overline{\mathbb{Q}})$ is in bijection with $S_F(\mathbb{C})$.

In order to establish the connection with Y, we choose a $\mathbb{Q}$-basis of F. This allows us to see an isomorphism of $\mathbb{A}_{F,f}$-modules $\psi : \mathbb{A}_{F,f} \to V(E)$ as an isomorphism of $\mathbb{A}_f$-modules ${\mathbb{A}_f}^2 \to V(E)$. Since the α is unique, we obtain an injection

$$S_F(\overline{\mathbb{Q}}) \hookrightarrow Y(\mathbb{C}), \quad {}_{\cong}\backslash(E(\overline{\mathbb{Q}}) \otimes \mathbb{Q}, \alpha, \psi) \mapsto {}_{\cong}\backslash(E(\overline{\mathbb{Q}}) \otimes \mathbb{Q}, \psi).$$

The points in the $\mathrm{GL}_2(\mathbb{A}_f)$-orbits of the images of this map for all F are called *CM-points* or *special points*.

Group actions on $S_F(\overline{\mathbb{Q}})$

Just as for $Y(\overline{\mathbb{Q}})$ we have a $G_F = G(\overline{\mathbb{Q}}|F)$-action on $S_F(\overline{\mathbb{Q}})$. We let only G_F and not $G_{\mathbb{Q}}$ act because the latter would possibly switch between different α.

Moreover, there also is an obvious ${\mathbb{A}_{F,f}}^\times$-action on it.

Proposition 4.3 *The group ${\mathbb{A}_{F,f}}^\times$ acts transitively on $S_F(\overline{\mathbb{Q}})$. The stabilizer of any element is $F^\times$.*

Proof. The transitivity is clear. For we have already pointed out that up to isogeny, there is only one elliptic curve with CM by F. So we can just choose one ψ, and obtain the others by multiplying with ${\mathbb{A}_{F,f}}^\times$.

Let now $x \in {\mathbb{A}_{F,f}}^\times$ be in the stabilizer of (E, α, ψ). This means that there is an element $\phi \otimes q \in \mathrm{End}(E) \otimes \mathbb{Q}$ such that $x\psi$ equals $V(\phi) \circ \psi$, where $V(\phi)$ stands for the induced map on $V(E)$. But that is, as we have seen before, precisely multiplication by some element in $F^\times$. Consequently, x is in $F^\times$, proving the claim. $\square$

The proposition can be reformulated by saying that $S_F(\overline{\mathbb{Q}})$ is an $F^\times\backslash\mathbb{A}_{F,f}^\times$-torsor. Explicitly, one has a bijection

$$F^\times\backslash\mathbb{A}_{F,f}^\times \overset{\text{bij.}}{\longleftrightarrow} S_F(\overline{\mathbb{Q}}) \quad g \mapsto \big((\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{F}/\mathcal{O}_F) \otimes \mathbb{Q}, \alpha, g\big),$$

where the α is the only (and evident) one.

Formulation of the main theorem of CM for elliptic curves

Write C_F for $F^\times\backslash\mathbb{A}_{F,f}^\times$. We have seen that there are actions by G_F and by C_F on $S_F(\overline{\mathbb{Q}})$, which commute. Our aim is to describe the G_F-action.

We will use the identification between $S_F(\overline{\mathbb{Q}})$ and C_F. In particular, we have a G_F-action on C_F.

Since $S_F(\overline{\mathbb{Q}})$ is a torsor of the commutative group C_F, we have a group homomorphism

$$\Phi : G_F^{ab} \to C_F, \quad \sigma \mapsto (\sigma.1).$$

Let us quickly check this. $\Phi(\sigma\tau) = \sigma.(\tau.1) = \sigma((\tau.1)1) = (\tau.1)(\sigma.1) = \Phi(\sigma)\Phi(\tau)$. Another way to say this is that $\sigma \in G_F^{ab}$ acts on $S_F(\overline{\mathbb{Q}})$ via multiplication with $\Phi(\sigma)$.

Now let us relate this homomorphism with class field theory. In the case of an imaginary quadratic field, class field theory provides an isomorphism, the *Artin map* or the *norm residue symbol*,

$$C_F \to G_F^{ab}.$$

Let's formulate the main theorem of complex multiplication for elliptic curves.

Theorem 4.4 *The composition of the Artin map with the homomorphism* Φ

$$C_F \xrightarrow{\text{Artin}} G_F^{ab} \xrightarrow{\Phi} C_F$$

sends $x \in C_F$ *to* x^{-1}.

Hence, $\sigma \in G_F^{ab}$ acts on an isomorphism class $(E \otimes \mathbb{Q}, \alpha, \psi)$ by multiplying ψ with the inverse of the image of σ under the inverse Artin map.

A Shimura variety like description of $S_F(\overline{\mathbb{Q}})$

Considering the fact that this is a seminar on Shimura varieties, I'd now like to mention a Shimura variety like desciption of C_F.

Robert has already mentioned the Weil restriction. We use it here and put

$$T = \mathrm{Res}_{\mathcal{O}_F/\mathbb{Z}} \mathbb{G}_{m,\mathcal{O}_F}.$$

It is a commutative group scheme over $\mathbb{Z}$ with the property

$$T(A) = (\mathcal{O}_F \otimes_{\mathbb{Z}} A)^\times$$

for all $\mathbb{Z}$-algebras A.

Let's calculate. $T(\mathbb{Q}) = (\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Q}) = F^\times$ and
$T(\mathbb{A}_f) = (\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{A}_f)^\times = (\mathcal{O}_F \otimes_{\mathbb{Z}} (\mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}))^\times = (F \otimes_{\mathbb{Z}} \hat{\mathbb{Z}})^\times = \mathbb{A}_{F,f}{}^\times$.

Consequently, we can write $C_F = T(\mathbb{Q}) \backslash T(\mathbb{A}_f)$.

The formalism of Shimura varieties will be treated by Theo in the next talk. Robert's and my talks were the motivation for doing the abstract theory...

A Appendix - A functorial point of view on Y

In this section we describe Y as a functor, making sense of $Y(S)$ for any $\mathbb{Q}$-scheme S. Of course, this functor is representable by the $\mathbb{Q}$-scheme Y that we have treated before. Furthermore, we shall exhibit a $\mathrm{GL}_2(\mathbb{A}_f)$-action on the points $Y(S)$, functorially for all allowed S, which gives us that the action is already defined over $\mathbb{Q}$.

This treatment was suggested by Bas Edixhoven. The idea is, however, also present in Deligne-Rapoport, IV.3.11, p. 74.

I should point out that I have not checked all the details. Moreover, I see that the exposition is not at all good, which makes understanding the actual ideas difficult. Maybe, I'll rewrite the appendix later.

Pontryagin duality

It seems to me that I need this paragraph on Pontryagin duality only because of a bad choice made before, which I will try to "correct" in this and the following paragraph. The aim is to replace $\hat{\mathbb{Z}}^2$ and $\varprojlim_n E[n]$ by the Pontryagin duals $(\mathbb{Q}/\mathbb{Z})^2$ and E_{tors} respectively.

Pontryagin duality is defined on the category $\mathcal{TAB}$ of topological abelian groups. One sets:

$$A^\vee = \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z}),$$

where one, of course, wants the homomorphisms to be continuous. One has that the dual of a discrete group is compact, that of a compact discrete. Moreover, the dual of a discrete torsion group is profinite and vice versa. In the case of a discrete torsion group, the $\mathbb{R}/\mathbb{Z}$ can be replaced by $\mathbb{Q}/\mathbb{Z}$ and the continuity assumption is empty.

Important for us are the two formulae: $(\mathbb{Q}/\mathbb{Z})^\vee = \hat{\mathbb{Z}}$ and $\hat{\mathbb{Z}}^\vee = \mathbb{Q}/\mathbb{Z}$.

Categorically, the principal theorem of Pontryagin duality can be formulated as follows.

Theorem A.1 *For all $A, B \in \mathcal{TAB}$ Pontryagin duality provides isomorphisms of abelian groups*

$$\mathrm{Hom}(A, B) \cong \mathrm{Hom}(B^\vee, A^\vee)$$

and

$$\mathrm{Isom}(A, B) \cong \mathrm{Isom}(B^\vee, A^\vee).$$

Let us now consider the category $\mathcal{TAB} \otimes \mathbb{Q}$, defined analogously to $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$. In it we also define a Pontryagin duality in the obvious way:

$$(A \otimes \mathbb{Q})^\vee = \mathrm{Hom}(A \otimes \mathbb{Q}, \mathbb{R}/\mathbb{Z} \otimes \mathbb{Q}) = \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q} = A^\vee \otimes \mathbb{Q}.$$

Proposition A.2 *For all $A \otimes \mathbb{Q}, B \otimes \mathbb{Q} \in \mathcal{TAB} \otimes \mathbb{Q}$ Pontryagin duality provides isomorphisms of abelian groups*

$$\mathrm{Hom}(A \otimes \mathbb{Q}, B \otimes \mathbb{Q}) \cong \mathrm{Hom}((B \otimes \mathbb{Q})^\vee, (A \otimes \mathbb{Q})^\vee)$$

and

$$\mathrm{Isom}(A \otimes \mathbb{Q}, B \otimes \mathbb{Q}) \cong \mathrm{Isom}((B \otimes \mathbb{Q})^\vee, (A \otimes \mathbb{Q})^\vee)$$

Proof. In fact, the proof is just a simple calculation, starting from "usual" Pontryagin duality: $\mathrm{Hom}(A, B) \cong \mathrm{Hom}(B^\vee, A^\vee)$. We tensor both sides with $\mathbb{Q}$ to get $\mathrm{Hom}(A \otimes \mathbb{Q}, B \otimes \mathbb{Q}) \cong \mathrm{Hom}(B^\vee \otimes \mathbb{Q}, A^\vee \otimes \mathbb{Q})$. But we have seen above that the right hand side is equal to $\mathrm{Hom}((B \otimes \mathbb{Q})^\vee, (A \otimes \mathbb{Q})^\vee)$ finishing this proof, since Isom is analogous. $\square$

Let us note another fact. The dual of $T(E)$, i.e. the projective limit over the $E[n]$ for an elliptic curve, is the injective limit over the $E[n]$, which I denote E_{tors}. If we are given $E \otimes \mathbb{Q}$ in $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$, we define $(E \otimes \mathbb{Q})_{\mathrm{tors}}$ to be $E_{\mathrm{tors}} \otimes \mathbb{Q}$.

Rewriting $Y(\mathbb{C})$

The first claim I make is that for any elliptic curve E over $\mathbb{C}$ the assignment $\phi \otimes q \mapsto (z \otimes r \mapsto \phi(z) \otimes rq)$ gives an isomorphism of $\mathbb{Q}$-vector spaces

$$\mathrm{Isom}_{\mathcal{TAB}}(\hat{\mathbb{Z}}^2, T(E)) \otimes \mathbb{Q} \cong \mathrm{Isom}_{\mathbb{A}_f-\mathrm{mod.}}(\hat{\mathbb{Z}}^2 \otimes \mathbb{Q}, T(E) \otimes \mathbb{Q}).$$

Since every element from the left space is of the form $\phi \otimes q$, the injectivity is clear. I still have to check the surjectivity.

From Pontryagin duality we now have isomorphisms of $\mathbb{Q}$-vector spaces

$$\begin{aligned}\mathrm{Isom}_{\mathbb{A}_f-\mathrm{mod}}(\hat{\mathbb{Z}}^2 \otimes \mathbb{Q}, T(E) \otimes \mathbb{Q}) &\cong \mathrm{Isom}_{\mathcal{TAB}}((\mathbb{Q}/\mathbb{Z})^2, E_{\mathrm{tors}}) \otimes \mathbb{Q} \\ &\cong \mathrm{Isom}_{\mathcal{TAB}\otimes\mathbb{Q}}\big((\mathbb{Q}/\mathbb{Z})^2 \otimes \mathbb{Q}, (E \otimes \mathbb{Q})_{\mathrm{tors}}\big).\end{aligned}$$

This establishes that the category $\mathrm{ShEll}(\mathbb{C})$ of pairs $(E \otimes \mathbb{Q}, \psi)$, which we have regarded earlier, with $E \otimes \mathbb{Q} \in \mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ and $\psi \in \mathrm{Isom}_{\mathbb{A}_f-\mathrm{mod}}(\hat{\mathbb{Z}}^2 \otimes \mathbb{Q}, T(E) \otimes \mathbb{Q})$, is the same as the one with ψ replaced by its image in $\mathrm{Isom}\big((\mathbb{Q}/\mathbb{Z})^2, (E \otimes \mathbb{Q})_{\mathrm{tors}}\big)$. We note that $\mathbb{Q}/\mathbb{Z}$ being discrete we can forget about continuity.

The same reasoning applies also to the category $\widehat{\mathrm{Ell}}(\mathbb{C})$ of pairs (E, ϕ) with $E \in \mathrm{Ell}(\mathbb{C})$ and $\phi : \hat{\mathbb{Z}}^2 \to T(E)$ an isomorphism of $\hat{\mathbb{Z}}$-modules. We obtain that ϕ can be replaced by its image in $\mathrm{Isom}\big((\mathbb{Q}/\mathbb{Z})^2, E_{\mathrm{tors}}\big)$.

The next claim is that the assignment $(E, \phi) \mapsto (E \otimes \mathbb{Q}, \phi \otimes 1)$ gives the bijection of sets

$$_{\cong}\backslash\widehat{\mathrm{Ell}}(\mathbb{C}) = {}_{\cong}\backslash\{\ (E, \phi)\ \} \ \overset{\text{bij.}}{\longleftrightarrow}\ {}_{\cong}\backslash\{\ (E \otimes \mathbb{Q}, \psi)\ \} = {}_{\cong}\backslash\mathrm{ShEll}(\mathbb{C}),$$

that I have already mentioned in part 2. Surjectivity should be clear, since any ψ is of the form $\phi \otimes 1/n$. A pair $(E \otimes \mathbb{Q}, \phi \otimes 1/n)$ is isomorphic to $(nE \otimes \mathbb{Q}, \phi \otimes 1)$. For the injectivity one has to check that any two isogenous elliptic curves with isomorphic Tate modules, are isomorphic. That sounds plausible.

Let us now consider the category $\mathcal{AB}_{\mathbb{N}}$ of injective systems of abelian groups indexed by $\mathbb{N}$, which we order by divisibility, with the obvious morphisms. A typical object of this category is $(\mathbb{Q}/\mathbb{Z})^2 = (\frac{1}{n}\mathbb{Z}/\mathbb{Z})^2_n$ with respect to the inclusions. For an elliptic curve we consider $E_{\mathrm{tors}} = (E[n])_n$, also with respect to the inclusions.

Of course, we can also take the category $\mathcal{AB}_{\mathbb{N}} \otimes \mathbb{Q}$. We define a new category, called $\widetilde{\mathrm{Ell}}(\mathbb{C})$, consisting of pairs $(E \otimes \mathbb{Q}, (\phi_n)_n \otimes \mathbb{Q})$, with $E \otimes \mathbb{Q} \in \mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ and $(\phi_n)_n \otimes \mathbb{Q}$ an isomorphism in the category $\mathcal{AB}_{\mathbb{N}}(\mathbb{C}) \otimes \mathbb{Q}$ between $(\mathbb{Q}/\mathbb{Z})^2 \otimes \mathbb{Q}$ and $(E \otimes \mathbb{Q})_{\mathrm{tors}} = E_{\mathrm{tors}} \otimes \mathbb{Q}$.

With these definitions, one has bijections

$$Y(\mathbb{C}) \xleftrightarrow{\text{bij.}} {}_{\cong}\backslash \mathrm{ShEll}(\mathbb{C}) \xleftrightarrow{\text{bij.}} {}_{\cong}\backslash \widetilde{\mathrm{Ell}}(\mathbb{C}).$$

Let us point out that we (still) have a $\mathrm{GL}_2(\mathbb{A}_f) = \mathrm{GL}_2(\hat{\mathbb{Z}}^2 \otimes \mathbb{Q})$-action on the injective systems (defined in the evident way).

Elliptic curves over $\mathbb{Q}$-schemes

We have up to this point reinterpreted $Y(\mathbb{C})$ as the isomorphism classes of a category, namely $\widetilde{\mathrm{Ell}}(\mathbb{C})$, that seems easier to generalise to arbitrary $\mathbb{Q}$-schemes (instead of $\mathbb{C}$). This generalisation shall be done now.

We want to use, of course, the results from last semester's seminar on modular curves, in which the Y_{K_n} were constructed to represent the moduli problem for elliptic curves with a full level n structure, making sense for every scheme over a given basis. Let us recall the definitions.

We define the category $\mathrm{Ell}_{\mathbb{Q}}$ to have as objects elliptic curves $E/S/\mathbb{Q}$, i.e. $E \to S$ a proper smooth morphism over $\mathrm{Spec}(\mathbb{Q})$, whose geometric fibres are connected smooth curves of genus 1, having an S-valued point 0. The morphisms are cartesian diagrams.

For such an $E/S \in \mathrm{Ell}_{\mathbb{Q}}$ one denotes by $E[n]_S$ the scheme theoretic kernel of multiplication by the integer n, which is an S-group scheme. For an elliptic curve $E/\mathbb{C}$, one finds that $E[n]_{\mathbb{C}}$ equals the constant $\mathbb{C}$-group scheme on the group of n-torsion points of $E(\mathbb{C})$.

A full level n structure in that setting is an isomorphism of S-group schemes $\phi_n : (\frac{1}{n}\mathbb{Z}/\mathbb{Z})_S \to E[n]_S$, where the left hand term stands for the constant group scheme.

We know from the geometry seminar last semester that there is a universal object $E^{\mathrm{univ}}_{K_n}/Y_{K_n}$ in the category $\mathrm{Ell}^n_{\mathbb{Q}}$ consisting of pairs $(E/S, \phi_n)$ with $E/S \in \mathrm{Ell}_{\mathbb{Q}}$ and ϕ_n a full level n structure.

One can obtain that the S-points of Y_{K_n} correspond to isomorphism classes in $\mathrm{Ell}^n_{\mathbb{Q}}(S)$, which is the category of pairs $(E/S, \phi_n)$ for a fixed scheme S.

We want to imitate the construction made above, and we define the category $\mathcal{AB}_{\mathbb{N}}(S)$ of injective systems of commutative S-group schemes in analogy with $\mathcal{AB}_{\mathbb{N}}$. Elements are e.g. $(\mathbb{Q}/\mathbb{Z})^2_S = \big((\frac{1}{n}\mathbb{Z}/\mathbb{Z})^2_S\big)_n$ and for an elliptic curve E/S the "torsion" $E_{\mathrm{tors},S} = \big(E[n]_S\big)_n$.

Now we want to introduce a generalisation $\widetilde{\mathrm{Ell}}_{\mathbb{Q}}(S)$ of $\widetilde{\mathrm{Ell}}(\mathbb{C})$ for affine $\mathbb{Q}$-schemes S. Objects are pairs $(E/S \otimes \mathbb{Q}, (\phi_n)_n \otimes \mathbb{Q})$ with $E/S \otimes \mathbb{Q}$ in $\mathrm{Ell}_{\mathbb{Q}}(S) \otimes \mathbb{Q}$ and $(\phi_n)_n \otimes \mathbb{Q}$ an isomorphism in $\mathcal{AB}_{\mathbb{N}}(S) \otimes \mathbb{Q}$ between $(\mathbb{Q}/\mathbb{Z})^2_S \otimes \mathbb{Q}$ and $E_{\mathrm{tors},S} \otimes \mathbb{Q}$.

It should now be possible to check that one thus obtains a bijection for a fixed affine $\mathbb{Q}$-scheme S

$$Y(S) \quad \overset{\text{bij.}}{\longleftrightarrow} \quad {}_{\cong}\backslash \widetilde{\mathrm{Ell}}_{\mathbb{Q}}(S).$$

The $\mathrm{GL}_2(\mathbb{A}_f)$-action

It is clear that we have a $\mathrm{GL}_2(\mathbb{A}_f) = \mathrm{GL}_2(\hat{\mathbb{Z}} \otimes \mathbb{Q})$-action on the set on the right, compatibly for $T \to S$. Namely, the constant group scheme $\mathrm{GL}_2(\hat{\mathbb{Z}})_S$ on S acts on the compatible system of full level n structures.

Yoneda's lemma applied in the category of affine $\mathbb{Q}$-schemes now implies that the group $\mathrm{GL}_2(\mathbb{A}_f)$ acts on the scheme Y, which was one of the aims of this appendix.

To conclude with, let us remark that the category $\widetilde{\mathrm{Ell}}_{\mathbb{Q}}(S) \otimes \mathbb{Q}$ has to be defined differently if S is not compact.