SHIMURA VARIETIES

YI HANG ZHU

Abstract. These notes are based on a topics course on Shimura varieties delivered by Yihang Zhu at the University of Maryland in Spring of 2022. Notes were taken by Steven Jin and edited by Y.Z.. If you have questions or corrections please contact Y.Z..

CONTENTS

A description of the course 3
Prerequisites 3
Useful references 3
1. Lecture 1 4
1.1. Modular curves 4
1.2. Higher dimensional generalizations 5
1.3. Adelic reformulation 6
2. Lecture 2 6
2.1. Continuation of the overview 6
3. Lecture 3 8
3.1. Characterization of the algebraic variety structure 8
3.2. Naive classification of elliptic curves over $\mathbb{C}$ 9
3.3. Alternative point of view: Hodge structures 10
4. Lecture 4 11
4.1. Classification of elliptic curves via Hodge structures 11
5. Lecture 5 13
5.1. Some motivation for level structure 13
5.2. Level structure 14
6. Lecture 6 15
6.1. Points on the modular curve 15
6.2. Variation of Hodge structures 16
7. Lecture 7 17
7.1. Variation of Hodge structures, continued 17
7.2. Families of elliptic curves 18
7.3. The moduli functor 19
8. Lecture 8 20
8.1. Proof of Proposition 7.3.3, continued 20
9. Lecture 9 22
9.1. Isomorphism between the algebraic and analytic moduli spaces 22
9.2. The representability of $S(N)$ 23
9.3. Generalities on relative curves 23
10. Lecture 10 24
10.1. Generalities on relative curves, continued 24
A description of the course

Shimura varieties play a vital role in the arithmetic aspects of the Langlands Program. This course will focus on the point of view that they are moduli spaces of abelian varieties with additional structures. Thus for most of the time we restrict our scope to the so-called PEL Shimura varieties. It will be important for us to treat these moduli spaces as schemes over a mixed characteristic base. Our aim is to survey some important arithmetic applications of these Shimura varieties after establishing their existence and basic properties.

A list of intended topics:

1. Modular curves and Siegel modular varieties over the complex numbers.
2. Siegel modular varieties as schemes: the representability of the moduli of principally polarized abelian varieties (following Mumford).
3. Shimura–Taniyama reciprocity law for CM abelian varieties; a glimpse into the theory of canonical models of Shimura varieties (preview of Prof. Rapoport’s course in the fall).
4. The PEL moduli problem, representability, and smoothness.
5. Number of points over a finite field and the relationship to the global Langlands correspondence.
6. Geometry of the mod $p$ Shimura variety and arithmetic applications. Topics should include the supersingular loci in some low dimension Shimura varieties, Ihara’s lemma, and applications such as congruences of modular forms.
7. If time permits, we have the following three directions in mind for further exploration. The actual choice will depend on the amount of time left as well as the interest of the audience:
   a. bad reduction (probably an example-based survey).
   b. towards Hodge-type and abelian-type Shimura varieties.
   c. relation with the geometric Satake equivalence (following Liang Xiao and Xin-wen Zhu).

We plan to spend the most time on the even-numbered topics.

Prerequisites. Basic understanding of algebraic geometry (such as Hartshorne’s textbook), algebraic number theory (adèles/ideles, the statements of class field theory), and abelian varieties (such as Mumford’s textbook) will be assumed. Along the way we will encounter $p$-divisible groups, some $p$-adic Hodge theory, some étale cohomology theory, and a lot of algebraic groups. We will try to cover the minimum background as much as possible. Some prior experience with modular curves and modular forms will be helpful but not strictly needed.

Useful references. (This list is to grow in the future)

- Elliptic curves and modular curves: The two volumes by Silverman [Sil09, Sil94] are the standard introductory textbooks on elliptic curves. A friendly introduction to modular curves is given in [DS05]. For more serious treatment that uses schemes systematically, see the book by Katz–Mazur [KM85], and the handouts in Brian Conrad’s course [Cond], especially [Con, Conc].
- Abelian varieties and their moduli: [Mum08], [MFK94], [GN06].
- For Shimura varieties, the original references for the modern perspective are Deligne’s two articles [Del71, Del79]. See also Milne’s notes [Mil17b] for a self-contained overview. (These references are, however, perhaps more relevant to Rapoport’s
course in the fall as opposed to the current one.) In [Lau], you can see the examples of many Shimura varieties.

- Our discussion of modular curves and Siegel modular varieties over $\mathbb{C}$ is similar in spirit to the first four chapters of Milne’s expository article [Mil11], which explains the relationship between Shimura varieties and moduli spaces.

1. Lecture 1

In this lecture we provide a brief motivational overview.

1.1. Modular curves. Let $\mathbb{H} = \{ z \in \mathbb{C} \mid \text{Im } z > 0 \}$. There is a left action of $SL_2(\mathbb{R})$ on $\mathbb{H}$, given as follows: for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ and $z \in \mathbb{H}$, we define

$$g \cdot z := \frac{az + b}{cz + d}$$

Note that this yields a surjection

$$SL_2(\mathbb{R}) \twoheadrightarrow \text{Aut}_{\text{hol}}(\mathbb{H})$$

where $\text{Aut}_{\text{hol}}(\mathbb{H})$ is the holomorphic automorphism group of $\mathbb{H}$. We are interested in certain discrete subgroups of $SL_2(\mathbb{R})$ whose actions will produce interesting quotients of $\mathbb{H}$.

Definition 1.1.1. We say that a subgroup $\Gamma \subset SL_2(\mathbb{Z})$ is a congruence subgroup if it is a subgroup $\Gamma \subset SL_2(\mathbb{Z})$ such that $\Gamma(N) \subset \Gamma$ with finite index for some $N \geq 1$, where

$$\Gamma(N) = \left\{ g \in SL_2(\mathbb{Z}) \mid g \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$  

We will also usually assume that $\Gamma$ is small enough, i.e., that $\Gamma \subset \Gamma(N)$ for some $N \geq 3$.

The group $\Gamma$ acts freely and properly discontinuously on $\mathbb{H}$, and this implies that $\Gamma \backslash \mathbb{H}$ has a canonical complex manifold structure given by the complex structure on $\mathbb{H}$. Furthermore, the quotient map $\mathbb{H} \to \Gamma \backslash \mathbb{H}$ is the universal covering.

Definition 1.1.2. The complex manifold $\Gamma \backslash \mathbb{H}$ is called a modular curve.

Proposition 1.1.3. A modular curve $\Gamma \backslash \mathbb{H}$ enjoys the following properties:

1. $\Gamma \backslash \mathbb{H}$ has the canonical structure of an algebraic variety over $\mathbb{C}$, which is compatible with the complex manifold structure.
2. $\Gamma \backslash \mathbb{H}$ is the moduli space of elliptic curves over $\mathbb{C}$ with “$\Gamma$-level structure”.
3. The moduli interpretation in (2) also makes sense over some number field $E$ (depending on $\Gamma$; e.g., $E = \mathbb{Q}(\zeta_N)$ if $\Gamma = \Gamma(N)$). This moduli problem over $E$ is then represented by a quasi-projective $E$-scheme whose base change to $\mathbb{C}$ recovers $\Gamma \backslash \mathbb{H}$ as a $\mathbb{C}$-scheme. We say that $\Gamma \backslash \mathbb{H}$ has a model over $E$.
4. The model over $E$ in (3) can be canonically characterized by using “special points” in $\Gamma \backslash \mathbb{H}$ and the Hecke action, without reference to the moduli problem.

Remark.

- The fact in (1) is not obvious, as the complex manifold $\Gamma \backslash \mathbb{H}$ is not compact. Hence, one cannot appeal to the usual equivalence between smooth projective curves over $\mathbb{C}$ and compact Riemann surfaces. The key is that there is a canonical compactification of $\Gamma \backslash \mathbb{H}$ which is a compact Riemann surface (the Baily–Borel compactification).
1.2. Higher dimensional generalizations. To obtain higher dimensional generalizations of the modular curves, we replace $\text{SL}_2$ by a reductive group $G$ over $\mathbb{Q}$. One key example to keep in mind is the \textbf{symplectic similitude group} $G = \text{GSp}_{2g}$. Recall that this is defined as follows. Fix a $2g$-dimensional symplectic vector space $V$ over $\mathbb{Q}$, that is, a vector space $V$ over $\mathbb{Q}$ equipped with a symplectic bilinear form $\langle - , - \rangle$. Then for any $\mathbb{Q}$-algebra $R$,

$$\text{GSp}_{2g}(R) = \text{GSp}(V)(R) = \{ g \in \text{GL}(V \otimes R) \mid \exists \nu(g) \in R^\times, \forall v, w \in V, \langle gv, gw \rangle = \nu(g) \langle v, w \rangle \}.$$ 

More informally, we write

$$\text{GSp}_{2g} = \{ g \in \text{GL}(V) \mid \exists \nu(g) \in \mathbb{G}_m, \forall v, w \in V, \langle gv, gw \rangle = \nu(g) \langle v, w \rangle \}.$$ 

Remark. Setting $g = 1$ gives $\text{GSp}_{2g} = \text{GL}_2$, not $\text{SL}_2$.

At the same time, we wish to generalize $\mathbb{H}$ to a (possibly disconnected) homogeneous space $X$ under a left action of the real Lie group $G(\mathbb{R})$ which admits a complex structure (invariant under the $G(\mathbb{R})$-action). We also require a Hermitian structure on each tangent space (invariant under the $G(\mathbb{R})$-action). This implies that there is constant curvature, which we insist must be negative. We require that $X$ cannot be too small by requiring that up to connected components $X$ is isomorphic to the \textbf{symmetric space} of $G^\text{ad}(\mathbb{R})$, i.e., the quotient of $G^\text{ad}(\mathbb{R})$ by a maximal compact subgroup.

Remark. For $G = \text{GL}_n$ with $n \geq 3$, there is no such $X$.

Fix such $G$ and $X$ as above. We wish to generalize the notion of a congruence subgroup to this setting.

Definition 1.2.1. We say that a subgroup $\Gamma \subset G(\mathbb{Q})$ is a \textbf{congruence subgroup} if $\Gamma$ contains $K \cap G(\mathbb{Q})$ with finite index for some compact open subgroup $K$ of $G(\mathbb{A}_f)$ where $\mathbb{A}_f$ is the finite adeles of $\mathbb{Q}$. We also assume that $\Gamma$ is “small enough”, or \textbf{neat}.

Remark. The (canonical) topology on $G(\mathbb{A}_f)$ can be described in the following elementary manner. Fix an injective $\mathbb{Q}$-homomorphism $\rho : G \rightarrow \text{GL}_n$ for some $n$. For each integer $N \geq 1$, define

$$K_{\rho,N} := \{ g \in G(\mathbb{A}_f) \mid \rho(g) \in \text{GL}_n(\mathbb{Z}) \subset \text{GL}_n(\mathbb{A}_f), \rho(g) \rightarrow 1 \in \text{GL}_n(\mathbb{Z}/NZ) \}.$$ 

For the fixed $\rho$ and varying $N$, the subgroups $K_{\rho,N}$ of $G(\mathbb{A}_f)$ are all open compact, and they form a neighborhood basis of 1. Thus a subgroup $\Gamma \subset G(\mathbb{Q})$ is a congruence subgroup if and only if it contains with finite index the inverse image under $\rho$ of some congruence subgroup of $\text{GL}_n(\mathbb{Q})$ (the latter defined in the same way as in the $\text{SL}_2$ case).

As in the modular curve case, for a neat congruence subgroup $\Gamma \subset G(\mathbb{Q})$, the set $\Gamma \backslash X$ can be canonically equipped with the structure of a complex manifold. This manifold enjoys similar properties as before.
Proposition 1.2.2.

- The complex manifold $\Gamma \backslash X$ can be given the structure of a quasi-projective complex variety (again thanks to the Baily–Borel compactification which is a projective complex variety containing $\Gamma \backslash X$ as a Zariski open).
- For some specific choices of $(G, X)$ (called of PEL type), we enjoy analogues of (2),(3), and (4) from Proposition 1.1.3, where in (2), the moduli of elliptic curves becomes the moduli of abelian varieties equipped with some additional structures.

1.3. Adelic reformulation. Fix a compact open subgroup $K \subset G(\mathbb{A}_f)$, which we also assume to be small enough, or neat.

Remark. We are omitting the definitions of neatness for now, but we note that the notion of neatness for compact open subgroups of $G(\mathbb{A}_f)$ is closely related to the neatness for congruence subgroups of $G(\mathbb{Q})$.

We define the set

$$\text{Sh}_K = G(\mathbb{Q}) \backslash X \times G(\mathbb{A}_f)/K.$$ 

Here $G(\mathbb{Q})$ acts diagonally on the left of $X \times G(\mathbb{A}_f)$ as follows:

- $G(\mathbb{Q})$ acts on $X$ via the action of $G(\mathbb{R})$ on $X$.
- $G(\mathbb{Q})$ acts on $G(\mathbb{A}_f)$ by left multiplication.

Here $K$ acts on the right of $X \times G(\mathbb{A}_f)$ by right multiplication on the factor $G(\mathbb{A}_f)$.

Notice that a priori $\text{Sh}_K$ is merely a set, and a rather unmanageable one at that. The following finiteness result assuages us.

Proposition 1.3.1 (Borel finiteness). The set $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)/K$ is finite.

We now equip $\text{Sh}_K$ with the structure of a smooth quasi-projective complex variety. Fix $g_1, \ldots, g_n \in G(\mathbb{A}_f)$ to be representatives of $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)/K$. For each $i$, let

$$\Gamma_i = G(\mathbb{Q}) \cap g_i K g_i^{-1},$$

where the intersection is taken inside $G(\mathbb{A}_f)$. As $K$ is neat, we know the $\Gamma_i$ are neat congruence subgroups of $G(\mathbb{Q})$.

Proposition 1.3.2. The map $\prod_{i=1}^n \Gamma_i \backslash X \to \text{Sh}_K$ given by sending $x \in \Gamma_i \backslash X$ to the double coset of $(x, g_i)$ is a bijection.

We leave the proof as an exercise.

We use the above bijection to equip $\text{Sh}_K$ with the structure of a smooth quasi-projective complex variety, i.e., the disjoint union of the $\Gamma_i \backslash X$. The resulting structure is independent of the choices of the representatives $g_i$.

Remark. The variety $\text{Sh}_K$ is disconnected in general, for two reasons:

- $X$ might be disconnected in general (although sometimes becomes connected after taking the quotient by $\Gamma_i$)
- We typically have $n \geq 2$.

2. Lecture 2

2.1. Continuation of the overview. We have indicated that we are interested in compact open subgroups $K \subset G(\mathbb{A}_f)$ that are neat. We show that there is a rich source of such subgroups.
Suppose $\rho: G \to \text{GL}_n$ is a faithful algebraic representation over $\mathbb{Q}$. This induces a morphism of topological groups

$$\rho: G(\mathbb{A}_f) \to \text{GL}_n(\mathbb{A}_f).$$

We have a subgroup

$$H := \{g \in \text{GL}_n(\mathbb{Z}) \mid g \mapsto 1 \text{ inside } \text{GL}_n(\mathbb{Z}/N\mathbb{Z})\} \subset \text{GL}_n(\mathbb{A}_f)$$

where $N \geq 1$. Then the $K_{\rho,N} := \rho^{-1}(H) \subset G(\mathbb{A}_f)$ are compact open subgroups that form a neighborhood basis of $1$, where $\rho$ is fixed and we vary $N$.

**Proposition 2.1.1** (Criterion for Neatness). If $K \subset G(\mathbb{A}_f)$ is a compact open subgroup such that $K \subset K_{\rho,N}$ for some $\rho$ and $N \geq 3$ as above, then $K$ is neat.

Let $K \subset G(\mathbb{A}_f)$ be a neat compact open subgroup. As in the previous lecture, we define the set $\text{Sh}_K$ as follows:

$$\text{Sh}_K = G(\mathbb{Q}) \setminus X \times G(\mathbb{A}_f)/K \cong \prod_{i=1}^n \Gamma_i \setminus X$$

where $\Gamma_i \subset G(\mathbb{Q})$ are congruence subgroups. The fact that $K$ is neat implies that the $\Gamma_i$ are also neat. This equips the set $\text{Sh}_K$ with the structure of a complex manifold.

Of course, we also desire the structure of an algebraic variety over $\mathbb{C}$ on $\text{Sh}_K$. *A priori*, there may be $0$ or $\geq 2$ possible ways to give a compatible variety structure on $\text{Sh}_K$ whose analytification is the underlying complex manifold. (If $\text{Sh}_K$ happens to be compact, then there is at most one way.) Nonetheless, there is in fact a canonical variety structure, coming from the Baily–Borel compactification: we are able to embed the complex manifold $\text{Sh}_K$ into a normal projective variety such that $\text{Sh}_K$ is a Zariski open set in said variety. In particular, $\text{Sh}_K$ has the canonical structure of a quasi-projective smooth variety. Moreover, this variety structure can be characterized by a universal property (and is in fact absolutely unique), to be discussed in the next lecture.

Next, the gist of Shimura varieties is that they can be (canonically) defined over number fields. For this, it is important to upgrade the pair $(G, X)$ to a Shimura datum in the sense of Deligne. This amounts to the extra datum of a $G(\mathbb{R})$-equivariant injective$^1$ map

$$X \hookrightarrow \text{Hom}_\mathbb{R}(S, G_{\mathbb{R}})$$

satisfying some axioms which we omit for now. Here, $S = \text{Res}_{C/\mathbb{R}}(G_m)$ is the Deligne torus, and $\text{Hom}_\mathbb{R}(S, G_{\mathbb{R}})$ is the set of $\mathbb{R}$-algebraic group homomorphisms $S \to G_{\mathbb{R}}$, on which $G(\mathbb{R})$ acts on by conjugation on $G_{\mathbb{R}}$.

The following theorem is a deep result due to the effort of numerous mathematicians.

**Theorem 2.1.2** (Shimura, Deligne, Milne, Borovoi, et al.). Fix a Shimura datum

$$(G, X, X \hookrightarrow \text{Hom}_\mathbb{R}(S, G_{\mathbb{R}})).$$

For each neat compact open subgroup $K \subset G(\mathbb{A}_f)$, $\text{Sh}_K$ has a canonical model over a canonical number field $E$. Here $E$, called the reflex field, depends only on the Shimura datum, not on $K$.

**Example.** We give an example of a Shimura datum. Let $G = \text{GL}_2$ and $X = \mathbb{H}^+ \bigsqcup \mathbb{H}^- = \mathbb{C} \setminus \mathbb{R}$. Define an $\mathbb{R}$-homomorphism $h: S \to G_{\mathbb{R}}$ as follows. For any $\mathbb{R}$-algebra $R$, we have

$$S(R) = (R \otimes \mathbb{R} \mathbb{C})^\times = \{a \otimes 1 + b \otimes i \mid a, b \in R, \ a^2 + b^2 \in R^\times\}.\footnote{For some purposes injectivity can be loosen to finite-to-one.}$$
We define $\mathbb{S}(R) \to G(R) = \text{GL}_2(R)$ by

$$a \otimes 1 + b \otimes i \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$ 

Now, note that $\text{GL}_2(\mathbb{R})/\text{SO}_2(\mathbb{R}) \cdot \mathbb{R}^\times \cong X$ under the map $g \mapsto g \cdot i$. (Here $\mathbb{R}^\times$ embeds into $\text{GL}_2(\mathbb{R})$ as the scalar matrices.) Then, we define

$$X \cong \text{GL}_2(\mathbb{R})/\text{SO}_2(\mathbb{R}) \cdot \mathbb{R}^\times \hookrightarrow \text{Hom}_R(\mathbb{S}, G_R)$$

via $g \mapsto \text{Int}(g) \circ h, \forall g \in \text{GL}_2(\mathbb{R})$, where $\text{Int}(g)$ is the inner automorphism $x \mapsto gxg^{-1}$ of $\text{GL}_2, \mathbb{R}$. In this case, the reflex field $E = \mathbb{Q}$.

In this course, we will mainly consider Shimura data such that the resulting Shimura varieties are closely related to certain moduli spaces of abelian varieties (with additional structures). More precisely, these Shimura varieties are isomorphic, up to disjoint unions, to such moduli spaces. Focusing on the moduli point of view will enable us to obtain good models over Zariski open sets of $\text{Spec} \mathcal{O}_E$, as opposed to just $\text{Spec} E$. Further, this will allow us to study the geometry and arithmetic of the reductions of the models modulo primes of $E$.

There are a number of applications along these lines.

1. The construction of Galois representations attached to certain automorphic forms, as predicted in the Langlands program: This began with Deligne in the 1960s-1970s, who attached 2-dimensional Galois representations to cuspidal eigenforms on $\text{GL}_2$ of weight $\geq 2$. This led to his famous resolution of the Ramanujan conjecture in this setting. A closely related problem is the computation of the Hasse–Weil zeta functions of these Shimura varieties. The prototype for this work is the Eichler–Shimura Theorem in the cases of modular curves and Shimura curves.

2. Congruences for modular forms: one critical exhibition of such an application is Ribet’s theorem, which played an important role in the resolution of Fermat’s Last Theorem.

Our first goals in this course, to be addressed in the next few lectures, are the following:

- Classify elliptic curves / abelian varieties with additional structure over $\mathbb{C}$ via modular curves in the one dimensional case and Siegel modular varieties in higher dimensions.
- Prove representability of the moduli functor of principally polarized abelian varieties (ppav) over $\mathbb{Z}$, following Mumford.

3. Lecture 3

3.1. Characterization of the algebraic variety structure. Let $(G, X)$ be a pair as in a Shimura datum. For this subsection, we do not require the datum of $X \hookrightarrow \text{Hom}_R(\mathbb{S}, G_R)$. Here we will use the classical language as opposed to the adelic language. For every neat congruence subgroup $\Gamma \subset G(\mathbb{Q})$, we recall that $\Gamma \backslash X$ is a complex manifold, with its structure inherited from the universal covering $X \to \Gamma \backslash X$. As before, the Bailey–Borel compactification provides an algebraic variety structure on $\Gamma \backslash X$ that is compatible with its complex manifold structure.

The following theorem gives a characterization of the algebraic variety structure in terms of the complex manifold structure.

**Theorem 3.1.1** (Borel). *For every smooth variety $S/\mathbb{C}$, every holomorphic map $S^{\text{an}} \to \Gamma \backslash X$ is algebraic, with respect to the algebraic structure on $\Gamma \backslash X$ given by Baily–Borel. In*
particular, there is in fact a unique algebraic variety structure on the complex manifold \( \Gamma \backslash X \).\(^2\)

3.2. Naive classification of elliptic curves over \( \mathbb{C} \). In this subsection, all algebraic varieties are over \( \mathbb{C} \). Recall that an elliptic curve \( E \) is a complete group variety of dimension one. We denote the identity element by \( O = O_E \in E(\mathbb{C}) = E \).

We now list some facts about elliptic curves which we will admit.

1. The group structure on an elliptic curve is automatically commutative.
2. If we have an algebraic morphism \( f : E \to E' \) between elliptic curves such that \( f(O_E) = O_{E'} \), then \( f \) is automatically a group homomorphism.
3. By a lattice in \( \mathbb{C} \) we mean a \( \mathbb{Z} \)-submodule of \( \mathbb{C} \) generated by an \( \mathbb{R} \)-basis of \( \mathbb{C} \). For each lattice \( \Lambda \subset \mathbb{C} \), we equip the compact Riemann surface \( \mathbb{C}/\Lambda \) with the group structure coming from addition on \( \mathbb{C} \). Since there is an equivalence of categories between compact Riemann surfaces and smooth projective algebraic curves, we see that \( (\mathbb{C}/\Lambda, +) \) is an elliptic curve.

Remark. We can in fact write down an explicit embedding \( \mathbb{C}/\Lambda \to \mathbb{P}_\mathbb{C}^1 \) using the Weierstrass \( \wp \) function and its derivative \( \wp' \).

4. Every elliptic curve arises as \( \mathbb{C}/\Lambda \) for some lattice \( \Lambda \subset \mathbb{C} \). More precisely, given an elliptic curve \( E \), there is a holomorphic group homorphism \( \exp : \text{Lie } E \to E \) coming from Lie group theory. Here \( \text{Lie } E \) is a 1-dimensional complex vector space. (Note that \( \exp \) is not algebraic.) Then \( \ker(\exp) \) is a lattice in \( \text{Lie } E \) and

\[
(\text{Lie } E)/\ker(\exp) \to E
\]

is an isomorphism of elliptic curves. Notice also that (non-canonically) the left hand side is isomorphic to \( \mathbb{C}/\Lambda \) for some lattice \( \Lambda \subset \mathbb{C} \).

Remark. The map \( \exp : \text{Lie } E \to E \) is a universal covering. Hence we have the following canonical isomorphisms:

\[
\ker(\exp) \cong \pi_1(E, O) \cong H^1(E, \mathbb{Z}).
\]

5. Suppose \( E \) and \( E' \) are elliptic curves. We have

\[
\text{Hom}(E, E') \to \{ f \in \text{Hom}(E, E') \mid f(\text{Lie } E) \cong H^1(E, \mathbb{Z}) \}
\]

where the assignment is given by

\[
F \mapsto dF|_{\text{Lie } E}.
\]

Combining the above facts, we have an equivalence of categories

\[
((V, \Lambda), V \text{ a 1-dim' } \mathbb{C} \text{-vector space and } \Lambda \subset V \text{ a } \mathbb{Z} \text{-lattice}) \to (\text{Elliptic curves})
\]

given by

\[
(V, \Lambda) \mapsto V/\Lambda,
\]

with the inverse functor

\[
E \mapsto (\text{Lie } E, H^1(E, \mathbb{Z})).
\]

\(^2\)For the last statement, use the following fact which is an easy consequence of Zariski’s Main Theorem: If \( k \) is an algebraically closed field of characteristic zero, then every bijective algebraic morphism between two (irreducible) varieties over \( k \), with the target normal, is an isomorphism. See for instance [Mil17a, Prop. 8.60].
In other words, \( \Lambda = \lambda \) from the equivalence of categories (3.1), we obtain a bijection

\[
\{ \text{Lattices inside } \mathbb{C} \}/\text{homothety} \overset{\sim}{\longrightarrow} \{ \text{Elliptic curves} \}/\text{isomorphism}.
\]

We now make the set on the left hand side more explicit. Set

\[ H^\pm := H^+ \bigcup H^- = \mathbb{C} \setminus \mathbb{R}. \]

For a lattice \( \Lambda \) in \( \mathbb{C} \), we pick a \( \mathbb{Z} \)-basis \( w_1, w_2 \in \mathbb{C}^\times \) of \( \Lambda \). Then \( w_1/w_2 \in H^\pm \). If we choose another \( \mathbb{Z} \)-basis \( \{ w'_1, w'_2 \} \) of \( \Lambda \), then there is a (unique) matrix \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{GL}_2(\mathbb{Z}) \) such that

\[
\begin{align*}
\frac{w_1}{w_2} &= \frac{aw'_1 + bw'_2}{cw'_1 + dw'_2} = a \left( \frac{w'_1}{w'_2} \right) + b, \\
\frac{w'_1}{w'_2} &= c \left( \frac{w'_1}{w'_2} \right) + d.
\end{align*}
\]

In other words, \( \frac{w_1}{w_2} \) and \( \frac{w'_1}{w'_2} \) are related by the \( \text{GL}_2(\mathbb{Z}) \)-action on \( H^\pm \). Thus every lattice \( \Lambda \subset \mathbb{C} \) has an invariant in \( \text{GL}_2(\mathbb{Z}) \setminus H^\pm \). This construction induces a bijection from the set of homothety classes of lattices in \( \mathbb{C} \) to the set \( \text{GL}_2(\mathbb{Z}) \setminus H^\pm \). Moreover, \( \text{GL}_2(\mathbb{Z}) \setminus H^\pm \cong \text{SL}_2(\mathbb{Z}) \setminus H^+ \). Thus we have proved the following theorem.

**Theorem 3.2.1.** There is a natural bijection

\[
\text{SL}_2(\mathbb{Z}) \setminus H^+ \overset{\sim}{\longrightarrow} \{ \text{Elliptic curves} \}/\text{isomorphism}
\]

sending the \( \text{GL}_2(\mathbb{Z}) \)-orbit of \( \tau \in H^+ \) to the isomorphism class of \( \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau \).

3.3. **Alternative point of view: Hodge structures.** In the previous subsection, we classified elliptic curves \( V/\Lambda \) up to isomorphism by morally fixing the complex vector space \( V \) and varying \( \Lambda \). As an alternative point of view, we may fix an abstract \( \mathbb{Z} \)-module \( \Lambda \), finite free of rank 2, and ask how we could vary the \( \mathbb{C} \)-structure. We elaborate this idea below.

As before, an elliptic curve is given by \( E \cong (\text{Lie } E)/H_1(E, \mathbb{Z}) \). Also, we have a canonical isomorphism of 2-dimensional \( \mathbb{R} \)-vector spaces:

\[
\text{Lie } E \cong H_1(E, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}.
\]

Notice of course that \( \text{Lie } E \) also has a complex structure. Thus in order to reconstruct \( E \), we need the abstract \( \mathbb{Z} \)-module \( H_1(E, \mathbb{Z}) \) together with a complex structure on the \( \mathbb{R} \)-vector space \( H_1(E, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \). In general, to define a complex structure on an \( \mathbb{R} \)-vector space \( V \), it suffices to define multiplication by \( i \) such that \( i^2 = -1 \). In other words, a complex structure on \( V \) is exactly an element \( J \in \text{End}_\mathbb{R}(V) \) such that \( J^2 = -1 \), and this element corresponds to scalar multiplication by \( i \).

**Definition 3.3.1.** An integral Hodge structure of elliptic type is a pair \( (\Lambda, J) \) where \( \Lambda \) is a finite free \( \mathbb{Z} \)-module of rank 2 and \( J \in \text{End}_\mathbb{R}(V) \) is a complex structure on \( \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \).

As such, we can rewrite the equivalence of categories (3.1) as the following equivalence of categories:

\[
(\text{Elliptic curves}) \overset{\sim}{\longrightarrow} (\text{integral Hodge structures of elliptic type}).
\]

In particular, we obtain a bijection on the level of isomorphism classes of both categories respectively. It is worth noting that there is a more general notion of a Hodge structure:
Definition 3.3.2. Fix a subring $R \subset \mathbb{R}$, usually taken to be $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$. An $R$-Hodge structure is a finitely generated $R$-module $\Lambda$ together with a direct sum decomposition

$$\Lambda \otimes_R \mathbb{C} = \bigoplus_{p,q \in \mathbb{Z}} F^{p,q}$$

as $\mathbb{C}$-vector spaces such that

$$\overline{F^{p,q}} \cong F^{q,p}.$$

Here the bar denotes the $\mathbb{R}$-linear automorphism of $\Lambda \otimes R \mathbb{C}$ (viewed as an $\mathbb{R}$-vector space) given by $x \otimes y \mapsto x \otimes \overline{y}, \forall x \in \Lambda, y \in \mathbb{C}$. In general, the type of a Hodge structure refers to the set of $(p,q)$ such that $F^{p,q} \neq 0$. We shall refer to this decomposition as the Hodge decomposition. The Hodge filtration refers to

$$\text{Fil}^i = \bigoplus_{p+q=i} F^{p,q}.$$

This is a decreasing filtration by $\mathbb{C}$-subspaces on $\Lambda \otimes_R \mathbb{C}$, i.e., we have $\text{Fil}^i \supset \text{Fil}^{i+1}$.

In light of this new language, we observe that there is an equivalence of categories:

(Integral Hodge structures of elliptic type) $\xrightarrow{\sim} (\mathbb{Z}$-Hodge structures free of rank 2 of type $\{-1,0\}$).

The assignment is as follows. Given an integral Hodge structure of elliptic type $(\Lambda, J)$, we define the decomposition $\Lambda \otimes \mathbb{Z} \mathbb{C} = F^{-1,0} \oplus F^{0,-1}$ by letting $F^{-1,0}$ and $F^{0,-1}$ be the eigenspaces for $\tilde{J}$ of eigenvalues $i$ and $-i$ respectively. Here $\tilde{J}$ denotes the $\mathbb{C}$-linear extension of $J \in \text{End}_\mathbb{R}(\Lambda \otimes \mathbb{R})$ to $\text{End}_\mathbb{C}(\Lambda \otimes \mathbb{Z} \mathbb{C}) = \text{End}_\mathbb{C}(\Lambda \otimes \mathbb{C})$. We leave it as an exercise for the reader to work out the construction in the reverse direction.

4. Lecture 4

4.1. Classification of elliptic curves via Hodge structures.

Definition 4.1.1. Let $R$ be a subring of $\mathbb{R}$, and $\Lambda$ an $R$-Hodge structure. We say that $\Lambda$ is pure of weight $m$ if in the direct sum decomposition $\Lambda \otimes R \mathbb{C} = \bigoplus_{p,q \in \mathbb{Z}} F^{p,q}$, all nonzero summands $F^{p,q}$ satisfy $p + q = m$.

Definition 4.1.2. Suppose $\Lambda$ is a $\mathbb{Z}$-Hodge structure, with Hodge decomposition $\Lambda \otimes \mathbb{Z} \mathbb{C} = \bigoplus_{p,q} F^{p,q}$. Let $\Lambda^* = \text{Hom}_{\mathbb{Z}\text{-mod}}(\Lambda, \mathbb{Z})$. Then we have $\Lambda^* \otimes \mathbb{Z} \mathbb{C} \cong \bigoplus_{p,q} (F^{p,q})^*$, where $*$ denotes the $\mathbb{C}$-linear dual. Define $G^{p,q} := F^{-p,-q}$. Then $\Lambda^* \otimes \mathbb{Z} \mathbb{C} = \bigoplus_{p,q} G^{p,q}$ is a Hodge decomposition. We thus obtain a $\mathbb{Z}$-Hodge structure $(\Lambda^*, (G^{p,q})_{p,q})$, which we call the dual of $\Lambda$.

Remark. Suppose $\Lambda$ is a Hodge structure pure of weight $m$. Then we can recover $F^{p,q}$ from $(\text{Fil}^i)_i$ and $m$, as

$$F^{p,q} = \text{Fil}^p \cap \overline{\text{Fil}^q}.$$

Recall that there is an equivalence of categories

(Elliptic curves) $\xrightarrow{\sim} (\text{Integral Hodge structures of elliptic type})$,

sending $E$ to $\Lambda = H_1(E, \mathbb{Z})$ with complex structure $J$ on $H_1(E, \mathbb{Z}) \otimes \mathbb{R} \cong \text{Lie} E$ given by that on $\text{Lie} E$. 
Remark. The usual Hodge decomposition

\[ \mathbf{H}^1(E, \mathbb{Z}) \otimes \mathbb{C} \cong \mathbf{H}^1(E, \mathbb{C}) \cong \mathbf{H}^0(E, \Omega^1_{E/\mathbb{C}}) \oplus \mathbf{H}^1(E, \mathcal{O}_E) \]

endows the \( \mathbb{Z} \)-module \( \mathbf{H}^1(E, \mathbb{Z}) \) with the structure of a \( \mathbb{Z} \)-Hodge structure of type \( \{(0,1), (1,0)\} \), where we set \( F^{0,1} = \mathbf{H}^1(E, \mathcal{O}_E) \) and \( F^{1,0} = \mathbf{H}^0(E, \Omega^1_{E/\mathbb{C}}) \). This Hodge structure is the dual of the integral Hodge structure of elliptic type that we attach to \( E \).

In summary, the task of classifying elliptic curves is tantamount to classifying integral Hodge structures of elliptic type up to isomorphism. But this is not so difficult. Since we identify isomorphic Hodge structures, notice that for any integral Hodge structure of elliptic type \( (\Lambda, J) \), we can choose a \( \mathbb{Z} \)-module isomorphism \( f : \Lambda \cong \mathbb{Z}^2 \). Then \( f \) transports \( J \) to a complex structure on \( \mathbb{Z}^2 \otimes \mathbb{R} = \mathbb{R}^2 \). In other words, we have a bijection

\[ \{ \text{Integral Hodge structures of elliptic type} \}/\text{isom} \cong \text{GL}_2(\mathbb{Z})/\{ \text{Complex structures on } \mathbb{R}^2 \} \]

where \( \text{GL}_2(\mathbb{Z}) \) acts by conjugation.

We now explain how this bijection is related to our previous bijection

\[ \text{GL}_2(\mathbb{Z})\backslash \mathbb{H}^\pm \cong \{ \text{Elliptic curves} \}/\text{isomorphism} \]

given by

\[ \tau \mapsto \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau). \]

Firstly, we have the following construction.

Proposition 4.1.3. There is a natural bijection

\[ \mathbb{H}^\pm \cong \{ \text{Complex structures on } \mathbb{R}^2 \}. \]

Proof. We first define the map. Recall that there is a \( \text{GL}_2(\mathbb{R}) \)-equivariant injection

\[ \mathbb{H}^\pm \hookrightarrow \text{Hom}_\mathbb{R}(\mathcal{S}, \text{GL}_2(\mathbb{R})) \]

where \( \mathcal{S} = \text{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m) \) is the Deligne torus. Note that an arbitrary element of \( \mathbb{H}^\pm \) can be described as \( \tau = g \cdot i \) where \( i \in \mathbb{H}^\pm \) is the base point and \( g \in \text{GL}_2(\mathbb{R})/\text{SO}_2(\mathbb{R}) \cdot \mathbb{R}^\times \).

The injection \( \mathbb{H}^\pm \hookrightarrow \text{Hom}_\mathbb{R}(\mathcal{S}, \text{GL}_2(\mathbb{R})) \) is defined by sending \( \tau = g \cdot i \) to the morphism \( h_{\tau} : \mathcal{S} \rightarrow \text{GL}_2(\mathbb{R}) \) of algebraic groups over \( \mathbb{R} \) defined as follows: for any \( \mathbb{R} \)-algebra \( T \), we can write \( \mathbb{S}(T) = (T \otimes_{\mathbb{R}} \mathbb{C})^\times = \{ a \otimes 1 + b \otimes i \mid a^2 + b^2 \in T^\times \} \).

The morphism \( h_{\tau} \) is defined via \( a \otimes 1 + b \otimes i \mapsto g \begin{pmatrix} a & b \\ -b & a \end{pmatrix} g^{-1} \). We then define

\[ \mathbb{H}^\pm \rightarrow \{ \text{Complex structures on } \mathbb{R}^2 \} \]

via \( \tau \mapsto J_{\tau} := h_{\tau}(i) \in \text{GL}_2(\mathbb{R}) \) where \( i \in \mathbb{C}^\times = \mathcal{S}(\mathbb{R}) \). It is an exercise to see that \( J_{\tau} \) is a complex structure and further that this assignment is a \( \text{GL}_2(\mathbb{R}) \)-equivariant bijection, where \( \text{GL}_2(\mathbb{R}) \) acts on \( \mathbb{H}^\pm \) by linear fractional transformations and \( \text{GL}_2(\mathbb{R}) \) acts on \( \{ \text{Complex structures on } \mathbb{R}^2 \} \) by conjugation. \( \square \)
**Proposition 4.1.4.** We have a string of bijections

\[
\begin{align*}
\{\text{Elliptic curves}\}/\text{isomorphism} \\
\{\text{Integral Hodge structures of elliptic type}\}/\text{isomorphism} \\
\text{GL}_2(\mathbb{Z})\setminus\{\text{Complex structures on } \mathbb{R}^2\} \\
\text{GL}_2(\mathbb{Z})\backslash \mathbb{H}^\pm \\
\text{SL}_2(\mathbb{Z})\backslash \mathbb{H}^+ 
\end{align*}
\]

where the third map is induced by the bijection \(\tau \mapsto J_\tau\) in the previous proposition. The composition of these maps is the inverse to \(\tau \mapsto \mathbb{C}/(\mathbb{Z} + \tau \mathbb{Z})\).

**Proof.** Exercise. \(\square\)

5. **Lecture 5**

5.1. **Some motivation for level structure.** Recall Proposition 4.1.4. In fact, we note that there is also an \(\text{SL}_2(\mathbb{Z})\)-invariant holomorphic morphism \(j : \mathbb{H}^+ \to \mathbb{C}\) inducing a bijection

\[
\text{SL}_2(\mathbb{Z})\backslash \mathbb{H}^+ \overset{\sim}{\to} \mathbb{C}.
\]

Here \(j\) corresponds to evaluating the classical \(j\)-invariant of an elliptic curve. We may use this map to identify the quotient \(\text{SL}_2(\mathbb{Z})\backslash \mathbb{H}^+\) with \(\mathbb{C}\) in order to give the former a complex manifold structure.

Note that \(\mathbb{H}^+ \to \text{SL}_2(\mathbb{Z})\backslash \mathbb{H}^+\) is a holomorphic map, but not a local isomorphism. In other words, this is not a covering map; there is ramification over the images of \(i\) and \(e^{\frac{2\pi i}{3}}\) with branching of order 2 and 3 respectively. This is related to the fact that the \(\text{SL}_2(\mathbb{Z})\)-action on \(\mathbb{H}^+\) is problematic in the following sense:

- \(-I \in \text{SL}_2(\mathbb{Z})\) acts trivially on \(\mathbb{H}^+\). In particular, the \(\text{SL}_2(\mathbb{Z})\)-action on \(\mathbb{H}^+\) is not free.
- The naive solution is to now consider the action of \(\text{SL}_2(\mathbb{Z})/\{\pm I\}\) on \(\mathbb{H}^+\). For this action, most points in \(\mathbb{H}^+\) have trivial stabilizer, but points in the orbit of \(i\) and the orbit of \(e^{\frac{2\pi i}{3}}\) have nontrivial stabilizers. So this is also not a solution.

This phenomenon exactly corresponds to the fact that for any elliptic curve \(E\) over \(\mathbb{C}\) (or any algebraically closed field of characteristic away from 2 or 3), the automorphism group of \(E\) is either:

1. \(\mathbb{Z}/2\mathbb{Z}\), where the nontrivial automorphism is negation. This corresponds to the inclusion of \(\{\pm I\}\) in all stabilizers.
2. \(\mathbb{Z}/4\mathbb{Z}\). This automorphism group applies to a unique isomorphism class of elliptic curves.
3. \(\mathbb{Z}/6\mathbb{Z}\). This automorphism group applies to a unique isomorphism class of elliptic curves.
Remark. The complex manifold structure we put on $\text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^+$ (using $j$) is the unique one such that the projection $\mathbb{H}^+ \to \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^+$ is holomorphic.

Remark. It is “more correct”, in some sense, to define the orbifold (or Deligne–Mumford stack) quotient of $\mathbb{H}^+$ by $\text{SL}_2(\mathbb{Z})$. This allows us to form a fine moduli space of elliptic curves that remembers the automorphisms (including the generic $\mathbb{Z}/2\mathbb{Z}$-automorphisms). As we will see in the future, the only obstruction to representability of the moduli of elliptic curves in the category of schemes is the presence of these automorphisms.

5.2. Level structure. Instead of seriously talking about orbifolds or stacks, we shall mainly focus on the following solution to the presence of automorphisms: we will rigidify the moduli problem by asking for some additional structures on the elliptic curves that will kill all automorphisms. In particular, no nontrivial automorphism of $E$ will preserve this extra structure. Correspondingly we will need to shrink $\text{SL}_2(\mathbb{Z})$ to some smaller congruence subgroup $\Gamma$ such that the $\Gamma$-action on $\mathbb{H}^+$ is free.

Fix an integer $N \geq 3$ throughout. For any elliptic $E$ over $\mathbb{C}$, consider the $N$-torsion subgroup

$$E[N] := \{ z \in E \mid z + \cdots + z \text{ (N times)} = 0 \}.$$  

Recall that $E[N]$ is non-canonically isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2 = \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ as $\mathbb{Z}/N\mathbb{Z}$-modules.

Definition 5.2.1. A choice of an isomorphism $\gamma : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ is called a level-$N$ structure on $E$. Equivalently, this is a choice of an ordered basis $(P, Q)$ of $E[N]$ as a free $\mathbb{Z}/N\mathbb{Z}$-module.

Recall that elliptic curves over $\mathbb{C}$ correspond to integral Hodge structures of elliptic type $(\Lambda, J)$. For an elliptic curve $E/\mathbb{C}$, the corresponding integral Hodge structure of elliptic type was obtained by setting $\Lambda = H_1(E, \mathbb{Z})$. We have the canonical isomorphisms

$$E[N] \cong \frac{1}{N} \Lambda/\Lambda \cong \Lambda/N\Lambda \cong \Lambda \otimes \mathbb{Z}/N\mathbb{Z}.$$  

It thus makes sense to formulate the following definition.

Definition 5.2.2. A level-$N$ structure on an integral Hodge structure of elliptic type $(\Lambda, J)$ is a choice of an isomorphism $\gamma : \Lambda/N\Lambda \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$.

Now, define

$$\Gamma(N) := \{ g \in \text{SL}_2(\mathbb{Z}) \mid g \equiv 1 \mod N \} \leq \text{SL}_2(\mathbb{Z}).$$  

The action of such groups on $\mathbb{H}^+$ behaves better than that of $\text{SL}_2(\mathbb{Z})$.

Proposition 5.2.3. For $N \geq 3$, $\Gamma(N)$ acts freely and properly discontinuously on $\mathbb{H}^+$.

Proof. We sketch the proof that the action is free. Suppose $\gamma \in \Gamma(N)$ has a fixed point in $\mathbb{H}^+$. Since the stabilizer of $i \in \mathbb{H}^+$ in $\text{SL}_2(\mathbb{R})$ is $\text{SO}_2(\mathbb{R})$ and since $\mathbb{H}^+$ is transitive under $\text{SL}_2(\mathbb{R})$, we see that $\gamma$ must lie in a $\text{SL}_2(\mathbb{R})$-conjugate of $\text{SO}_2(\mathbb{R})$. In particular $\gamma$ must be semi-simple and its eigenvalues in $\mathbb{C}$ have absolute value 1. On the other hand, the characteristic polynomial of $\gamma$ is monic with integer coefficients, so the eigenvalues of $\gamma$ are algebraic integers. Combined with the previous fact, we see that the eigenvalues of $\gamma$ must be roots of unity. Pick a prime power $p^r$ dividing $N$, and we can arrange that $p^r \geq 3$. Since $\gamma \equiv 1 \mod p^r$, each eigenvalue $\lambda$ of $\gamma$ in $\overline{\mathbb{Q}}_p$ must satisfy $v_p(\lambda - 1) \geq e$. We leave it as an exercise to the reader to show that any root of unity $\lambda \in \overline{\mathbb{Q}}_p$ satisfying $v_p(\lambda - 1) \geq e$ must be trivial provided that $p^r \geq 3$. Thus the eigenvalues of $\gamma$ are trivial, so $\gamma$ must be trivial.

We omit the proof that $\Gamma(N)$ acts properly discontinuously. See [DS05, §2.1]. \qed
In particular, this implies that $\Gamma(N)\backslash \mathbb{H}^+$ has the natural structure of a Riemann surface and $\mathbb{H}^+ \to \Gamma(N)\backslash \mathbb{H}^+$ is a covering. Further, this is obviously the universal covering, since $\mathbb{H}^+$ is simply connected.

**Definition 5.2.4.** The modular curve $Y(N)$ is the complex manifold

$$Y(N) := \bigsqcup_{j \in (\mathbb{Z}/N\mathbb{Z})^*} \Gamma(N)\backslash \mathbb{H}^+_j$$

where $\mathbb{H}^+_j := \mathbb{H}^+$.

**Remark.** Classically, the notation $Y(N)$ refers to just a single connected component $\Gamma(N)\backslash \mathbb{H}^+_\gamma$.

For each $j \in (\mathbb{Z}/N\mathbb{Z})^*$, fix once and for all an element $g_j \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\det(g_j) = j$. For instance, we may take $g_j = \begin{pmatrix} j & 0 \\ 0 & 1 \end{pmatrix}$.

For each $j \in (\mathbb{Z}/N\mathbb{Z})^*$ and each $\tau \in \mathbb{H}^+$, we will define an integral Hodge structure of elliptic type together with a level-$N$ structure:

$$V_\tau = (\Lambda_\tau, J_\tau, \gamma_\tau : \Lambda_\tau/NA_\tau \sim \to (\mathbb{Z}/N\mathbb{Z})^2)$$

as follows:

- $\Lambda_\tau := \mathbb{Z}^2$.
- $J_\tau$ is the complex structure on $\mathbb{R}^2$ corresponding to $\tau$, i.e., $J_\tau := h_\tau(i)$.
- $\gamma_\tau : \Lambda_\tau/NA_\tau \sim \to (\mathbb{Z}/N\mathbb{Z})^2$ is the isomorphism defined by $g_j : (\mathbb{Z}/N\mathbb{Z})^2 \sim \to (\mathbb{Z}/N\mathbb{Z})^2$. (By the definition of $\Lambda_\tau$, $\Lambda_\tau/NA_\tau$ is $(\mathbb{Z}/N\mathbb{Z})^2$.)

Observe that if $\tau, \tau' \in \mathbb{H}^+_\gamma$ are related by the $\Gamma(N)$-action, then $(\Lambda_\tau, J_\tau, \gamma_\tau) \cong (\Lambda_{\tau'}, J_{\tau'}, \gamma_{\tau'})$, i.e., there is an isomorphism of integral Hodge structures compatible with the level structures. In turn, we get a map

$$Y(N) \to \{\text{Integral Hodge structures of elliptic type with level-$N$ structure}/\text{isomorphism}\}.$$  

In the next lecture we will show that this map is a bijection.

6. Lecture 6

6.1. Points on the modular curve.

**Proposition 6.1.1.** The map (5.1) is a bijection.

**Proof.** We leave injectivity as an exercise. For surjectivity, let $V = (\Lambda, J, \gamma)$ be an arbitrary integral Hodge structure of elliptic type together with a level $N$-structure. Pick a group isomorphism $u : \Lambda \sim \to \mathbb{Z}^2$. Then $u$ takes $J$ to some complex structure on $\mathbb{Z}^2 \otimes_\mathbb{Z} \mathbb{R} = \mathbb{R}^2$, which must be of the form $J_\tau$ for some $\tau \in \mathbb{H}^\gg$. If $\tau \in \mathbb{H}^\ll$, we compose $u$ with some element of $\text{GL}_2(\mathbb{Z})$ of determinant $-1$, and as a result we can always assume that $\tau \in \mathbb{H}^\gg$. Now let $\gamma'$ be the composition

$$(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{u^{-1} \mod N} \Lambda/NA \xrightarrow{\gamma} (\mathbb{Z}/N\mathbb{Z})^2.$$  

Then $\gamma' \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We note the following fact:

**Fact.** (Strong approximation for $\text{SL}_2$.) The natural map $\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.

For a proof, see [DS05, Exercise 1.2.2]. Note that the statement is not true if we replace $\text{SL}_2$ by $\text{GL}_2$, since elements of $\text{GL}_2(\mathbb{Z})$ all have determinants $\pm 1$.

Let \( j = \det(\gamma') \), so \( \gamma' q_j^{-1} \in SL_2(\mathbb{Z}/N\mathbb{Z}) \). By the above fact, we can compose \( u \) with a suitable element of \( SL_2(\mathbb{Z}) \) to arrange that \( \gamma = g_j \). When we do this the element \( \tau \) we found in the above will be moved by the element of \( SL_2(\mathbb{Z}) \), but the new \( \tau \) still lies in \( \mathbb{H}^+ \). We think of it as an element of \( \mathbb{H}^+ \). It is then easy to check that \( u \) induces an isomorphism between \( V \) and \( V_\tau \). Thus the image of \( \tau \) under (5.1) is the isomorphism class of \( V \). \qed

**Corollary 6.1.2.** Points on \( Y(N) \) are in natural bijection with the isomorphism classes of elliptic curves with level \( N \)-structure.

**Remark.** Classically, one considers only one connected component of \( Y(N) \), and correspondingly imposes a stronger condition on the level \( N \)-structure. For this, recall that for each elliptic curve \( E \), the **Weil pairing** is a canonical isomorphism of \( \mathbb{Z}/N\mathbb{Z} \)-modules \( \Lambda_E^2 E[N] \simto \mu_N \). (Here \( \Lambda^2 \) is taken in the category of finite free \( \mathbb{Z}/N\mathbb{Z} \)-modules, and \( \mu_N \) is the set of \( N \)-th roots of unity in \( \mathbb{C} \).) Thus any level-\( N \) structure on \( E \) will induce an isomorphism between \( \mu_N \) and \( \Lambda_E^2(\mathbb{Z}/N\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z} \), or equivalently the choice of a generator of \( \mu_N \). If one insists that the level structure must induce a prescribed generator of \( \mu_N \), then under the correspondence one sees only one connected component of \( Y(N) \). It turns out that the generator \( e^{2\pi i/N} \) corresponds to the connected component \( \Gamma(N) \backslash \mathbb{H}^+ \). The verification of the last claim amounts to the explicit computation of the Weil pairing for \( \mathbb{C}/\mathbb{Z} + \tau \mathbb{Z} \) as in [Sil94, Exercise 1.15].

Up to this point, we just described how points on \( Y(N) \) correspond to isomorphism classes of elliptic curves or integral Hodge structures of elliptic type with level-\( N \) structure. We have not used the complex manifold structure or complex algebraic variety structure on \( Y(N) \). We would now like to upgrade the pointwise correspondence to a moduli interpretation. Recall that the complex manifold \( Y(N) \) has a unique compatible structure of an algebraic variety, by the theorems of Baily–Borel and Borel. The following is our target theorem.

**Theorem 6.1.3.** The algebraic variety \( Y(N) \) is the moduli space of elliptic curves with level-\( N \) structure. Namely, it represents the functor sending each finite-type \( \mathbb{C} \)-scheme \( V \) to the set of isomorphism classes of proper flat families of elliptic curves over \( V \) with level-\( N \) structure.

We will explain the notions in the statement of the theorem in more detail later.

### 6.2. Variation of Hodge structures

One important ingredient towards the proof of the Theorem 6.1.3 is the correct notion of a “family of integral Hodge structures of elliptic type”. Suppose \( S \) is a complex manifold and for each \( s \in S \) we are given an integral Hodge structure of elliptic type \((\Lambda_s, J_s)\). The question is how to formulate that these structures vary nicely as \( s \) varies in \( S \). In particular, we need to take into account the complex manifold structure on \( S \). The answer is provided in the following definition.

**Definition 6.2.1.** A variation of integral Hodge structures of elliptic type on \( S \) refers to a pair \((\Delta, \mathcal{L})\) consisting of a locally constant sheaf of abelian groups \( \Delta \) on \( S \) that is locally free of rank 2 over \( \mathbb{Z} \), and a holomorphic line subbundle \( \mathcal{L} \) of the plane bundle \( \Delta \otimes_{\mathbb{Z}} \mathcal{O}_S \). (Here \( \mathcal{O}_S \) is the structure sheaf of holomorphic functions on \( S \).) They should satisfy the following condition:

- For each \( s \in S \), the 1-dimensional \( \mathbb{C} \)-subspace of \( \Lambda_s \otimes_{\mathbb{Z}} \mathbb{C} \) determined by the fiber of \( \mathcal{L} \) is theFilp associated with a Hodge structure of elliptic type on \( \Lambda_s \) (i.e., a complex structure of elliptic type (\( \Lambda_s \), \( J_s \)). Suppose \( \mathbb{Z} \) is the stalk of \( \Lambda \) at \( s \), and we identify \( \Lambda_s \otimes_{\mathbb{Z}} \mathbb{C} \) with the fiber of the plane bundle \( \Delta_s \otimes_{\mathbb{Z}} \mathcal{O}_S \) at \( s \). Thus the fiber of \( \mathcal{L} \) at \( s \) gives rise to a subspace.
structure on $\Lambda_s \otimes \mathbb{Z} \mathbb{R}$, or equivalently a Hodge decomposition $\Lambda_s \otimes \mathbb{Z} \mathbb{C} = F^{-1,0} \oplus F^{0,-1}$ such that $F^{-1,0} = F^{0,-1}$).

Recall that for Hodge structures of elliptic type, or more generally pure Hodge structures, the Hodge decomposition and the Hodge filtration determine each other. Thus the above definition is equivalent to the datum of $\Lambda_s$ together with a Hodge structure of elliptic type on $\Lambda_s$ for each $s \in S$ such that the pointwise $\text{Fil}^0$’s vary holomorphically in the sense that they come from some holomorphic line subbundle $L \subset \Lambda \otimes \mathcal{O}_S$.

The following is the more general definition.

**Definition 6.2.2.** Let $R$ be a subring of $\mathbb{R}$, and let $m$ be an integer. A variation of $R$-Hodge structures of weight $m$ on $S$ refers to a pair $(\Lambda, L^\bullet)$, where $\Lambda$ is a locally constant sheaf of $R$-modules on $S$ that is locally finite free, and $L^\bullet$ is a decreasing filtration on $\Lambda \otimes \mathcal{O}_S$ by holomorphic sub-vector bundles. They should satisfy the following two conditions:

- For each $s \in S$, the filtration on the $\mathbb{C}$-vector space $\Lambda_s \otimes \mathbb{C}$ determined by the fibers of $L^\bullet$ at $s$ is the Hodge filtration associated with a (unique) Hodge structure of weight $m$ on $\Lambda_s$.

- (Griffiths transversality.) Let $\nabla : \Lambda \otimes \mathcal{O}_S \to \Lambda \otimes \Omega^1_S$ be the flat connection $\text{id} \otimes d$. For each $p$, we have $\nabla(L^p) \subset L^{p-1} \otimes \Omega^1_S$.

Note that for Hodge structures of elliptic type, Griffiths transversality is automatic.

If we have a smooth projective variety $X$ over $\mathbb{C}$, then for each non-negative integer $m$ we have the Hodge decomposition from Hodge theory:

$$H^m(X, \mathbb{Z}) \otimes \mathbb{C} = H^m(X, \mathbb{C}) = \bigoplus_{p+q=m} H^q(X, \Omega^p_X).$$

This makes $H^m(X, \mathbb{Z})$ a $\mathbb{Z}$-Hodge structure of weight $m$ (with $F^{p,q} = H^q(X, \Omega^p_X)$). The following result is the motivation for the definition of a variation of Hodge structures.

**Theorem 6.2.3 (Griffiths).** Let $X$ and $S$ be smooth algebraic varieties over $\mathbb{C}$, and let $X \to S$ be a smooth projective morphism. Then the Hodge structures on $H^m(X_s, \mathbb{Z})$ for $s \in S$ come from a canonical variation of $\mathbb{Z}$-Hodge structures of weight $m$ on $S^{an}$.

As a special case, we obtain the following

**Theorem 6.2.4.** Let $S$ be a smooth algebraic variety over $\mathbb{C}$, and let $E \to S$ be a proper flat family of elliptic curves. Then the integral Hodge structures of elliptic type assigned to $E_s$ for $s \in S$ come from a canonical variation of integral Hodge structures of elliptic type on $S^{an}$.

This is indeed a special case of Griffiths’ theorem, since the integral Hodge structure of elliptic type attached to an elliptic curve $E$ over $\mathbb{C}$ is the dual of $H^1(E, \mathbb{Z})$, and since $E \to S$ is automatically projective (i.e., after Zariski localization on $S$, it factors through $E \to \mathbb{P}^1_S$; a fact that is not true for higher dimensional abelian varieties). In fact, after Zariski localization on $S$, one can always find an $S$-embedding $E \hookrightarrow \mathbb{P}^1_S$ that is described by a Weierstrass equation. (More details in the future.)

## 7. Lecture 7

### 7.1. Variation of Hodge structures, continued.

We briefly recall some notions from before.
Definition 7.1.1. Let $S$ be a complex manifold. A variation of integral Hodge structures of elliptic type over $S$ is a pair $(\Lambda, J)$ where:

- $\Lambda$ is a locally constant sheaf of $\mathbb{Z}$-modules on $S$ that is locally free of rank 2 over $\mathbb{Z}$.
- $J = (J_s)_{s \in S}$ is a family where each $J_s$ is a complex structure on the $\mathbb{R}$-vector space $\Lambda_s \otimes \mathbb{R}$ such that $\text{Fil}^0(\Lambda_s \otimes \mathbb{C}) = (F^0)_{s}$ varies holomorphically in the sense that they all come from a holomorphic line sub-bundle $L$ of the plane bundle $\Lambda \otimes \mathcal{O}_S$.

Remark. Remembering $(\Lambda, J)$ is the same as remembering $(\Lambda, L)$.

Definition 7.1.2. By a level-$N$ structure on a variation of integral Hodge structures of elliptic type $(\Lambda, J)$, we mean a choice of sheaf isomorphism (as sheaves of groups)

$$\gamma : \Lambda \otimes \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2.$$  

Remark. Such an isomorphism need not exist in general!

7.2. Families of elliptic curves.

Definition 7.2.1. Let $S$ be a scheme. An elliptic curve over $S$ is a proper and smooth morphism of schemes $\pi : E \to S$, with geometric fibers that are (smooth and) connected curves of genus 1, along with the datum of a section $e : S \to E$.

Theorem 7.2.2 ("Abel", see [KM85, §2.1]). In the notation from the above definition, there is a canonical structure of an $S$-group scheme on $E$ with $e : S \to E$ the identity section. Moreover, this group scheme is commutative.

This group scheme structure is given similarly to the case where $S = \text{Spec} \ k$, with $k$ a field. For any $S$-scheme $T$, we will make $E(T)$ a group as follows. Write $f$ for the structural morphism $E \to S$, and let $f_T$ be the pullback of $f$ over $T$:

$$
\begin{array}{ccc}
E_T & \longrightarrow & E \\
\downarrow \quad f_T & & \downarrow f \\
T & \longrightarrow & S.
\end{array}
$$

For $P \in E(T)$, denote by $D_P$ the Cartier divisor on $E_T$ given by $\text{im}(P)$. (Thus $\mathcal{O}_{E_T}(D_P)$ is the invertible $\mathcal{O}_{E_T}$-module that is inverse to the ideal sheaf of $\text{im}(P)$.) Write $e_T$ for the section of $E_T \to T$ induced by $e$. Then for any $P, Q, R \in E(T)$, we impose that

$$P + Q = R$$

if and only if

$$\mathcal{O}_{E_T}(D_P) \otimes \mathcal{O}_{E_T}(D_Q) \cong \mathcal{O}_{E_T}(D_Q) \otimes \mathcal{O}_{E_T}(D_R) \otimes f^*_T(L)$$

for a line bundle $L$ on $T$.

Remark. The attribution to Abel rests in his classical proof that for an elliptic curve $E$ over $\mathbb{C}$ we have

$$E \sim \text{Jac}(E) = \{ \text{deg 0 divisors on } E \}/\text{linear equivalence}$$

via $P \mapsto [D_P - D_e]$.
Proposition 7.2.3 ([KM85, §2.3]). Suppose $E/S$ is an elliptic curve. After localizing $S$, the map $E \to S$ is projective. More precisely, each point in $S$ has an open neighborhood $U$ such that $E_U \to U$ factors through an embedding $E_U \to \mathbb{P}^2_U$ whose image is described by a generalized Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_i \in \mathcal{O}_U(U).$$

Remark. Projectivity over the base (even after localization) is not true for general abelian schemes; this is a special phenomenon about elliptic curves.

Corollary 7.2.4. Suppose $S$ is a smooth variety over $\mathbb{C}$ and $E/S$ is an elliptic curve. The pointwise integral Hodge structures of elliptic type associated to $E_s$ for $s \in S(\mathbb{C})$ come from a variation of integral Hodge structures of elliptic type over $S_{an}$. (More precisely, the local system in the variation of integral Hodge structures is the $\mathbb{Z}$-linear dual of the first derived pushforward of $\mathbb{Z}$ along $E_{an} \to S_{an}$.)

Definition 7.2.5. A (naive) level-$N$ structure on an elliptic curve $E/S$ is a choice of isomorphism of $S$-group schemes $\gamma : E[N] \sim \rightarrow (\mathbb{Z}/N\mathbb{Z})^2$.

Remark. In general, $E[N]$ is a finite locally free $S$-group of rank $N^2$. We will only consider the case when $N$ is invertible on $S$, i.e., $S$ is over $\mathbb{Z}[1/N]$. In this case $E[N]$ is finite étale over $S$, and after a finite étale base change $E[N]$ is isomorphic to the constant group scheme $(\mathbb{Z}/N\mathbb{Z})^2$.

Let $S$ be a $\mathbb{Z}[1/N]$-scheme, and $E/S$ an elliptic curve. Using the above remark, it is an exercise to show that giving a level $N$-structure on $E/S$ is the same as providing an ordered pair of sections $P$ and $Q$ of the $S$-scheme $E[N]$ such that for each geometric point $\bar{s}$ in $S$, the fibers of $P$ and $Q$ at $\bar{s}$ generate the group $E_{\bar{s}}[N]$.

Remark. There is an obvious version of Corollary 7.2.4 incorporating level-$N$ structure.

7.3. The moduli functor.

Theorem 7.3.1. Suppose $N \geq 3$. We define the contravariant functor $S(N) : \text{finite-type schemes over } \mathbb{Z}[1/N] \rightarrow (\text{sets})$ by

$$S \mapsto \{\text{isomorphism classes of elliptic curves } E/S \text{ with level-}N \text{ structure}\}.$$  

(On morphisms, this functor is defined by the obvious notion of pullback.) Then $S(N)$ is representable by a nice—in particular, finite type—scheme over $\mathbb{Z}[1/N]$, still denoted by $S(N)$.

Recall that by the Bailey–Borel compactification the complex manifold $Y(N)$ has a unique structure of an algebraic variety over $\mathbb{C}$.

Theorem 7.3.2. $S(N)_C$ is canonically isomorphic to $Y(N)$.

We will indicate the proof of Theorem 7.3.1 using explicit manipulation with Weierstrass equations in the near future. Later we will prove it again by deducing it from Mumford’s more general theorem for the moduli of abelian schemes. We now explain the proof of Theorem 7.3.2. For this we will first prove the following proposition.
Proposition 7.3.3. The complex manifold $Y(N)$ represents the contravariant functor

$\text{(complex manifolds)} \to \text{(sets)}$

sending $S$ to the set of isomorphism classes of variations of $\mathbb{Z}$-Hodge structures of elliptic type with level-$N$ structure on $S$. (On morphisms, this functor is defined by the obvious notion of pullback.)

Proof. Recall that for each $\tau \in Y(N)$, we have constructed an integral Hodge structure of elliptic type with level-$N$ structure $\mathcal{V}_\tau$ which is well defined up to isomorphism; see the map (5.1). We want to construct a variation of integral Hodge structures of elliptic type with level-$N$ structure on $Y(N)$ that recovers this pointwise construction. In the rest of the proof, we abbreviate “variation of integral Hodge structures of elliptic type with level $N$-structure” simply as “VHSL”.

Let $j \in (\mathbb{Z}/N\mathbb{Z})^\times$. Recall that we have fixed $g_j \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\det(g_j) = j$. First, we construct a VHSL on $\mathbb{H}_j^+$. Namely, we define

$$\widetilde{\mathcal{V}}_j = (\mathbb{Z}^2, (J_\tau)_{\tau \in \mathbb{H}_j^+}, \gamma : \mathbb{Z}^2 \otimes \mathbb{Z}/N\mathbb{Z} = (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{g_j} (\mathbb{Z}/N\mathbb{Z})^2).$$

Here, as always, $J_\tau$ denotes $h_\tau(i) \in \text{GL}_2(\mathbb{R})$. To show that $\widetilde{\mathcal{V}}_j$ is indeed a variation of Hodge structures, consider the map $\iota : \mathbb{H}_j^+ \to \mathbb{P}^1(\mathbb{C})$ sending $\tau \in \mathbb{H}_j^+$ to the 1-dimensional subspace $\text{Fil}^0 \subset \mathbb{C}^2$ determined by $J_\tau$ (i.e., the $-i$-eigenspace of the complexification of $J_\tau$). One checks that $\iota$ is the standard open embedding $\mathbb{H}_j^+ = \mathbb{C} - \mathbb{R} \to \mathbb{P}^1(\mathbb{C})$. This shows that the pointwise Fil$^0$’s in $\widetilde{\mathcal{V}}_j$ indeed vary holomorphically; more precisely, they come from the tautological line bundle on $\mathbb{P}^1(\mathbb{C})$ restricted to $\mathbb{H}_j^+$.

Now, suppose we have two points $\tau, \tau' \in \mathbb{H}_j^+$ related by some (unique) $g \in \Gamma(N)$. Say $\tau' = g\tau$. Then for any open neighborhood $U$ of $\tau$ in $\mathbb{H}_j^+$, we have an isomorphism

$$\widetilde{\mathcal{V}}_j|_U \simeq g^*(\widetilde{\mathcal{V}}_j|_{g(U)})$$

between VHSL’s on $U$ given by $g^{-1} : \mathbb{Z}^2 \xrightarrow{\sim} \mathbb{Z}^2$. (Exercise: check that this indeed preserves the other structures.) These isomorphisms satisfy the cocycle relation and give rise to a descent datum from $\mathbb{H}_j^+$ to $\Gamma(N)\backslash \mathbb{H}_j^+$, by which we obtain a VHSL on $\Gamma(N)\backslash \mathbb{H}_j^+$, denoted by $\mathcal{V}_j$. Note here that the local system in $\mathcal{V}_j$ is no longer constant, but rather its monodromy group is $\Gamma(N)$, which is the full fundamental group of $\Gamma(N)\backslash \mathbb{H}_j^+$. Taking disjoint union over the $j \in (\mathbb{Z}/N\mathbb{Z})^\times$, we obtain $\mathcal{V}^{\text{univ}}$ on $Y(N)$.

In the next lecture, we will show that $\mathcal{V}^{\text{univ}}$ is the universal VHSL. $\square$

8. Lecture 8

8.1. Proof of Proposition 7.3.3, continued.

Proof. It remains to show that $\mathcal{V}^{\text{univ}}$ is the universal VHSL. This amounts to showing that for any complex manifold $S$ and any VHSL $\mathcal{V}$ on $S$, there exists a unique holomorphic map $f : S \to Y(N)$ such that $\mathcal{V} \cong f^*\mathcal{V}^{\text{univ}}$. By Proposition 6.1.1, we have a bijection

$$Y(N) \to \{\text{Integral Hodge structures of elliptic type with level $N$ structure}\}/\text{isomorphism}.$$  

One checks that this bijection is exactly given by sending $\tau \in Y(N)$ to the isomorphism class of $(\mathcal{V}^{\text{univ}})_\tau$. This implies that the desired map $f$ must send each $s \in S$ to the unique $f(s) \in Y(N)$ such that $(\mathcal{V}^{\text{univ}})_{f(s)}$ is isomorphic to $\mathcal{V}_s$. Thus we know that $f$ is unique.

We must still check that $f$ given by the above recipe is holomorphic and $f^*\mathcal{V}^{\text{univ}} \cong \mathcal{V}$. If we wish to show that $f$ is holomorphic at $s_0 \in S$, then we may shrink $S$ to an open
neighborhood of $s_0$, which we may assume is connected and simply connected. This is always possible, since $S$ is just a complex manifold. In particular, after shrinking, we may assume that the local system in $V$ is constant. We denote

$$V = (\Lambda, (J_s)_{s \in S}, \gamma : \Lambda \otimes \mathbb{Z}/N\mathbb{Z} \rightarrow (\mathbb{Z}/N\mathbb{Z})^2).$$

Pick an isomorphism $\Lambda \cong \mathbb{Z}^2$. Then $\gamma$ becomes an element of $GL_2(\mathbb{Z}/N\mathbb{Z})$. Here $(J_s)_{s \in S}$ becomes a family of elements $(\tau_s)_{s \in S}$ where $\tau_s \in \mathbb{H}^\pm$. Using the fact that $\text{Fil}^0$ varies holomorphically, we know that $S \rightarrow \mathbb{H}^\pm$ given by $s \mapsto \tau_s$ is holomorphic. As such, the image of $S \rightarrow \mathbb{H}^\pm$ is either in $\mathbb{H}^+$ or $\mathbb{H}^-$, and in particular we may compose the selected isomorphism $\Lambda \cong \mathbb{Z}^2$ with a matrix in $GL_2(\mathbb{Z})$ with determinant $-1$ if necessary in order to assume that $S \rightarrow \mathbb{H}^\pm$ lands in $\mathbb{H}^+$.

Now recall that strong approximation for $SL_2$ says that $SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. In turn, we may further compose the isomorphism $\Lambda \cong \mathbb{Z}^2$ by an element of $SL_2(\mathbb{Z})$ if necessary to ensure that this isomorphism carries

$$\gamma : \Lambda \otimes \mathbb{Z}/N\mathbb{Z} \rightarrow (\mathbb{Z}/N\mathbb{Z})^2$$

to $g_j$ for some $j$.

After these adjustments, we get a holomorphic map $\tilde{f} : S \rightarrow \mathbb{H}^+_j$ such that for all $s \in S$, we have $V_s \cong (\tilde{V}_j)_{f(s)}$. We have a commutative diagram

$$\begin{array}{ccc}
\mathbb{H}^+_j & \downarrow \\
S & \rightarrow & Y(N).
\end{array}$$

Note here that $S$ has been shrunk to be connected and simply connected; of course such a lifting cannot be produced for general $S$. This implies that $f$ is holomorphic since $\tilde{f}$ is holomorphic.

Now we need that $f^*V^\text{univ}$ is isomorphic to $V$. First, we shrink $S$ to an open neighborhood of any given point in $S$, and we construct $\tilde{f}$ as before. Then, on any such neighborhood, we have

$$V \cong f^*(\tilde{V}_j) \cong f^*V^\text{univ}$$

where the first isomorphism can be checked using the construction of $\tilde{f}$ and the second isomorphism follows from the above commutative diagram. In other words, we have an open covering $(U_i)_{i \in I}$ of $S$ such that for each $i$, there is an isomorphism

$$\varphi_i : V|_{U_i} \cong (f^*V^\text{univ})|_{U_i}.$$ 

This yields our claim locally. Now we note the following fact.

**Fact 8.1.1.** For $N \geq 3$, on any complex manifold any VHSL has no automorphisms.

**Proof.** Let $S$ be a complex manifold and $V$ a VHSL on $S$. We may assume that $S$ is connected. Then any automorphism of $V$ is uniquely determined by its behavior at one fiber (since it is after all an automorphism of a local system). Thus we reduce to the case where $S$ is a point. In other words, we need to show that any integral Hodge structure of elliptic type with level-$N$ structure $(\Lambda, J, \gamma)$ has no automorphism. Suppose $g$ is an automorphism. Choose an identification $\Lambda \cong \mathbb{Z}^2$. Then $g$ becomes an element of $GL_2(\mathbb{Z})$. Since $g$ preserves $\gamma$, $g$ lies in $\Gamma(N)$. Since $g$ preserves $J$, $g$ has a fixed point in $\mathbb{H}^\pm$. But $\Gamma(N)$ acts freely on $\mathbb{H}^\pm$ (Proposition 5.2.3), so $g = 1$. \qed
This fact implies that on nontrivial intersections $U_i \cap U_j$, the isomorphisms $\varphi_i$ and $\varphi_j$ must agree; else $\varphi_i^{-1} \circ \varphi_j$ is a nontrivial automorphism of $V|_{U_i \cap U_j}$. Thus we can glue together the isomorphisms $\varphi_i$ to get a global isomorphism $\varphi : V \to f^*V_{univ}$. □

9. Lecture 9

9.1. Isomorphism between the algebraic and analytic moduli spaces. Recall the following two theorems from before. Let $N$ be an integer $\geq 3$.

**Theorem 9.1.1.** We define a contravariant functor

$$S(N) : (\text{finite type } \mathbb{Z}[1/N]\text{-schemes}) \to (\text{Sets})$$

given by

$$T \mapsto \{\text{iso. cl. of elliptic curves over } T \text{ with level-}N\text{ structure}\}.$$ 

Then $S(N)$ is representable by a “nice” $\mathbb{Z}[1/N]$-scheme, also denoted by $S(N)$. In particular, $S(N)_\mathbb{C}$ is a smooth $\mathbb{C}$-variety.⁴

**Theorem 9.1.2.** We have a natural isomorphism of $\mathbb{C}$-varieties

$$S(N)_\mathbb{C} \cong Y(N).$$

We will prove Theorem 9.1.2 assuming Theorem 9.1.1.

**Proof.** We write “VHSL” for “variation of integral Hodge structures of elliptic type with level-$N$ structure”. For any smooth $\mathbb{C}$-variety $T$, by the version of Corollary 7.2.4 incorporating level-$N$ structures, we have a functor

$$(\text{elliptic curves over } T \text{ with level-}N\text{ structure}) \to (\text{VHSL on } T_{\text{an}}).$$

In particular, we have a natural map between the sets of isomorphism classes. By Proposition 7.3.3 and Theorem 9.1.1, this is tantamount to a map

$$\text{Hom}_{\mathbb{C}\text{-sch}}(T, S(N)_\mathbb{C}) \to \text{Hom}_{\text{hol}}(T_{\text{an}}, Y(N)).$$

Consider the universal case, i.e., $T = S(N)_\mathbb{C}$. Then the distinguished element of the left hand side—namely, the identity—gives rise to a distinguished holomorphic map $f : S(N)^{\text{univ}}_\mathbb{C} \to Y(N))$. By Borel’s Theorem, $f$ is algebraic. Moreover, $f$ is a bijection on $\mathbb{C}$-points, since the induced map on $\mathbb{C}$-points is the familiar bijection

$$\{\text{isom. cl. of elliptic curves with level-}N\text{ structure}\}$$

$$\to \{\text{isom. cl. of integral Hodge structures of elliptic type with level-}N\text{ structure}\}.$$ 

**Fact 9.1.3.** Suppose $k$ is an algebraically closed field of characteristic 0 and $f : X \to Y$ is a morphism of $k$-varieties. If $Y$ is normal and $f$ is a bijection on $k$-points, then $f$ is an isomorphism.

This fact implies that $f : S(N)_\mathbb{C} \to Y(N)$ is an isomorphism of $\mathbb{C}$-varieties, since the target is smooth and a *a fortiori* normal. □

⁴Here and below, by a variety over an algebraically closed field $k$ we mean a reduced finite-type $k$-scheme such that each connected component is irreducible. Thus we allow a finite disjoint union of what are usually called $k$-varieties.
9.2. **The representability of** \( S(N) \). We will discuss the strategy first. Suppose that \( S \) is a scheme and \( E/S \) is an elliptic curve. By the Riemann–Roch Theorem, we will be able to construct “meromorphic functions with controlled poles”. From this we will attain Weierstrass coordinates on \( E \) locally on \( S \), i.e., after shrinking \( S \), we will find a closed \( S \)-embedding

\[
E \longrightarrow \mathbb{P}^2_S
\]

given by a Weierstrass equation

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.
\]

(The indexing is such that every term \( a_i x^j y^k \) satisfies \( i + 2j + 3k = 6 \).) The level-\( N \) structure on \( E \), which is used to rigidify the abstract elliptic curve, will serve to rigidify the concrete Weierstrass equation, in the sense that ambiguous choices of \( a_i \) for the same elliptic curve will be rigidified. Then, we will construct \( S(N) \) as the spectrum of \( \mathbb{Z}[1/N][a_i] \) modulo some relations.

In fact, we will only be able to do this explicitly for small values of \( N \). We will do this for \( N = 3 \) and \( N = 4 \), and then bootstrap the general case from \( S(3) \) and \( S(4) \). Namely, in the general case, this is done after passing through the open cover \{ \text{Spec } \mathbb{Z}[1/N] \cap \text{Spec } \mathbb{Z}[1/3], \text{Spec } \mathbb{Z}[1/N] \cap \text{Spec } \mathbb{Z}[1/4] \} \text{ of Spec } \mathbb{Z}[1/N].

**Remark.** In [KM85], instead of a construction of \( S(3) \) and \( S(4) \), they construct \( S(3) \) and a rigidified version of \( S(2) \). (Note that elliptic curves with level-2 structure always have automorphism group \( \mathbb{Z}/2\mathbb{Z} \), the non-trivial element being negation.) The construction for the rigidified version of \( S(2) \) in fact contains a mistake, as pointed out in [Conc, §2]. As a correction, one should just construct \( S(3) \) and \( S(4) \) instead. We will only explain the construction of \( S(3) \). The construction of \( S(4) \) as well as the explanation of the mistake in [KM85] are left as a presentation topic. The main reference is [Conc].

9.3. **Generalities on relative curves.** We collect some general facts about relative curves. Suppose \( S \) is a locally noetherian scheme. Suppose \( f : X \to S \) is a proper, smooth morphism of schemes whose geometric fibers are all connected of dimension 1. We also assume that \( f \) admits a section \( P : S \to X \), which we fix. We note that \( P \) is always a closed immersion. We write \( \mathcal{I}_P \) for the ideal sheaf of \( \text{im}(P) \) in \( X \).

**Facts:**

1. The \( \mathcal{O}_X \)-module \( \mathcal{I}_P \) is invertible. More precisely for all \( s \in S \), after shrinking \( S \) near \( s \), we can find an open neighborhood \( U \) of \( \text{im}(P) \) in \( X \) and \( t \in \mathcal{O}_U(U) \) such that \( \mathcal{I}_P|_U = t \cdot \mathcal{O}_U \) and \( t : \mathcal{O}_U \to \mathcal{O}_U \) is injective. This implies that \( \mathcal{I}_P \) is invertible. We shall call \( t \) a **local coordinate near** \( P \). When \( U \) is fixed, the choice of \( t \) is unique up to multiplication by \( \mathcal{O}_U(U) \).

   Let \( n \) be a positive integer. We will write \( \mathcal{O}(nP) \) for \( \mathcal{I}_P^{-n} \), a line bundle on \( X \). This is the “sheaf of functions that are allowed to have a pole of order \( n \) along \( P \)”. After choosing a local coordinate as above and shrinking \( U \) around \( \text{im}(P) \) in \( X \), we get an element \( t^{-1} \in \mathcal{O}(P)(U) \) such that \( \mathcal{O}(P) = t^{-1} \cdot \mathcal{O}_U \) and \( \mathcal{O}(nP) = t^{-n} \mathcal{O}_U \) for all \( n \in \mathbb{Z} \).

2. We have a natural map of \( \mathcal{O}_S \)-modules “taking the \( -n \)-th coefficient of the Laurent expansion at \( P \)"

\[
\text{Lead}_n : f_* \mathcal{O}(nP) \longrightarrow P^*(\Omega_{X/S})^{-n}.
\]

Here we note that \( \Omega_{X/S} \) is a line bundle on \( X \) thanks to our assumptions, so \( P^* \Omega_{X/S} \) is a line bundle on \( S \) and its negative tensor powers are defined.
10. Lecture 10

10.1. Generalities on relative curves, continued. We maintain the same assumptions as the previous section. Namely, suppose $S$ is a locally noetherian scheme. Fix $f : X \to S$ to be a proper smooth morphism of schemes with all geometric fibers connected of dimension 1. Fix a section $P \in X(S)$. We will describe the morphism of $\mathcal{O}_S$-modules

$$\text{Lead}_n : f_*\mathcal{O}(nP) \to P^*(\Omega_{X/S})^\otimes -n.$$  

First, we will provide an abstract description that does not rely on a choice of a local coordinate. Note that by adjunction, there is a natural map

$$f_*\mathcal{O}(nP) \to f_*P^*\mathcal{O}(nP) = P^*\mathcal{O}(nP).$$

So it suffices to define $P^*\mathcal{O}(nP) \to P^*(\Omega_{X/S})^\otimes -n$. Observe that we have the following string of isomorphisms of $\mathcal{O}_X/\mathcal{I}_P = \mathcal{O}_S$-modules:

$$P^*\mathcal{O}(nP) = P^*(\mathcal{I}_P^{-n}) = \mathcal{I}_P^{-n} \otimes_{\mathcal{O}_X} \mathcal{O}_X/\mathcal{I}_P = \mathcal{I}_P^{-n}/\mathcal{I}_P^{1-n} = (\mathcal{I}_P^{-1}/\mathcal{O}_X)^\otimes n.$$  

(The last $n$-th tensor power is over $\mathcal{O}_S$.)

It suffices to define an $\mathcal{O}_S$-module map

$$\mathcal{I}_P^{-1}/\mathcal{O}_X \to P^*(\Omega_{X/S})^\otimes -1,$$

or equivalently, an $\mathcal{O}_S$-bilinear pairing

$$\mathcal{I}_P^{-1}/\mathcal{O}_X \otimes_{\mathcal{O}_S} P^*\Omega_{X/S} \to \mathcal{O}_S.$$  

Now as a general fact (see [Sta18, Tag 0474]), $P^*\Omega_{X/S}$ is canonically identified with the conormal sheaf of $\text{im}(P)$ in $X$, namely $\mathcal{I}_P/\mathcal{I}_P^2$ viewed as an $\mathcal{O}_X/\mathcal{I}_P = \mathcal{O}_S$-module. The identification $\mathcal{I}_P/\mathcal{I}_P^2 \xrightarrow{\sim} P^*\Omega_{X/S}$ is given by $a \mapsto da$. Then, we define the pairing

$$\mathcal{I}_P^{-1}/\mathcal{O}_X \otimes_{\mathcal{O}_S} \mathcal{I}_P/\mathcal{I}_P^2 \to \mathcal{O}_S$$

by multiplication followed by reduction modulo $\mathcal{I}_P$.

For concreteness, we now also describe our morphism $\text{Lead}_n$ explicitly after choosing a local coordinate. Thus assume we have an open neighborhood $U$ of $\text{im}(P)$ in $X$ and a local coordinate $t \in \mathcal{O}_U(U)$ such that $t : \mathcal{O}_U \to \mathcal{O}_U$ is injective and $\mathcal{I}_P|_U = t \cdot \mathcal{O}_U$ as before. Then, we have

$$f_*\mathcal{O}(nP) = (\mathcal{I}_P^{-1}/\mathcal{O}_X)^\otimes n = (t^{-1}\mathcal{O}_U/\mathcal{O}_U)^\otimes n$$

viewed as $\mathcal{O}_U/t\mathcal{O}_U = \mathcal{O}_S$-modules. Also, we have

$$P^*\Omega_{X/S} = \mathcal{I}_P/\mathcal{I}_P^2 = t\mathcal{O}_U/t^2\mathcal{O}_U = (\mathcal{O}_U/t\mathcal{O}_U) \cdot dt|_{t=0} = \mathcal{O}_S \cdot dt|_{t=0}.$$  

Here the symbol $dt|_{t=0}$ denotes the image of $t$ in $t\mathcal{O}_U/t^2\mathcal{O}_U$, and $\mathcal{O}_S \cdot dt|_{t=0}$ is a rank 1 free $\mathcal{O}_S$-module generated by $dt|_{t=0}$. Finally, our pairing for $n = 1$ can be described as

$$(t^{-1}\mathcal{O}_U/\mathcal{O}_U) \otimes_{\mathcal{O}_S} \mathcal{O}_S \cdot dt|_{t=0} \to \mathcal{O}_S$$

via

$$(t^{-1}\zeta, \epsilon dt) \mapsto \zeta \epsilon \mod t.$$  

Remark. For more clarity, we can ask what the picture looks like in the classical case. Suppose $S = \text{Spec } k$ where $k$ is an algebraically closed field. Then $f_*\mathcal{O}(nP) = H^0(X, \mathcal{O}(nP))$ is the $k$-vector space consisting of $\zeta \in k(X)$ allowed to have a pole of at worst order $n$ at $P$ and regular at all other points. On the other side, we have $(P^*\Omega_{X/S})^\otimes -n = (\mathcal{I}_P X)^\otimes_{k,-n},$
where $T^*_pX$ is the cotangent space of $X$ at $P$. After choosing a local coordinate $t$ near $P$, we have $\mathcal{O}_{X,P} = k[[t]]$. We have the composition
\[ f_\ast \mathcal{O}(nP) \to k(X) \to \text{Frac} \mathcal{O}_{X,P} = k((t)) \]
which we think of as taking the Laurent expansion of a function $\zeta \in f_\ast \mathcal{O}(nP)$ at $P$. Also, $T^*_pX$ is a 1-dimensional $k$-vector space with a basis $dt|_{t=0}$ arising from the choice of $t$. Then the pairing is defined by sending $(\zeta, dt^{\otimes n})$ to the $-n$-th coefficient of the Laurent expansion of $\zeta$ at $P$.

10.2. More generalities: cohomology and base change. Suppose $f : X \to S$ is an arbitrary proper morphism of schemes, with $S$ locally noetherian. Suppose $\mathcal{F}$ is a coherent sheaf of $\mathcal{O}_X$-modules flat over $\mathcal{O}_S$, i.e., for all $x \in X$, the stalk $\mathcal{F}_x$ (which is an $\mathcal{O}_{X,x}$-module) is flat over $\mathcal{O}_{S,f(x)}$. For each $s \in S$, we write $X_s$ for the fiber of $X$ over $s$, namely the fiber product
\[
\begin{array}{ccc}
X_s & \longrightarrow & X \\
\downarrow & & \downarrow \\
\text{Spec } k(s) & \longrightarrow & S,
\end{array}
\]
Write $\mathcal{F}|_{X_s}$ for the pullback of $\mathcal{F}$ along $X_s \to X$.

Theorem 10.2.1. The following statements hold.

1. (See [MFK94, §0.5] or [Conb, Cor. 1.2, Prop. 2.1].) Suppose $H^1(X_s, \mathcal{F}|_{X_s}) = 0$ for all $s \in S$. Then $f_\ast \mathcal{F}$ is a vector bundle over $S$, and $R^1 f_\ast \mathcal{F} = 0$. Moreover, the formation of $f_\ast \mathcal{F}$ commutes with arbitrary base change in the following sense. Suppose $S'$ is locally noetherian and $g : S' \to S$ is an arbitrary morphism. Define $f' : X' \to S'$ to be the pullback of $f$ along $g$, i.e., we have the cartesian diagram
\[
\begin{array}{ccc}
X' & \longrightarrow & X \\
\downarrow & & \downarrow f \\
S' & \longrightarrow & S
\end{array}
\]
Let $\mathcal{F}'$ be the pullback of $\mathcal{F}$ to $X'$. Then the natural map (the “base change map”) of $\mathcal{O}_{S'}$-modules
\[ g^* f_\ast \mathcal{F} \longrightarrow f'_\ast \mathcal{F}' \]
is an isomorphism.

As a special case, we can take $g$ to be the map $\text{Spec}(k(s)) \to S$ defined by a point $s \in S$. Then the natural map of $k(s)$-vector spaces
\[ (f_\ast \mathcal{F}) \otimes_{\mathcal{O}_s} k(s) \longrightarrow H^0(X_s, \mathcal{F}|_{X_s}) \]
is an isomorphism. In particular, this means that any $k(s)$-basis of $H^0(X_s, \mathcal{F}|_{X_s})$ can be lifted to a trivialization of the vector bundle $f_\ast \mathcal{F}$ near $s \in S$.

2. (See [Conb, Thm. 1.1, Prop. 2.1].) Suppose for each $s \in S$, the natural map
\[ (f_\ast \mathcal{F}) \otimes_{\mathcal{O}_s} k(s) \longrightarrow H^0(X_s, \mathcal{F}|_{X_s}) \]
is surjective. Then the map is an isomorphism for each $s \in S$. Moreover, $f_\ast \mathcal{F}$ is a vector bundle, and the formation of $f_\ast \mathcal{F}$ commutes with arbitrary base change.
11. Lecture 11

11.1. Application: pushforward of the structure sheaf. As an application of Theorem 10.2.1 (2) above, we have the following useful result (cf. [Conb, Cor. 1.3]).

**Proposition 11.1.1.** Let $S$ be a locally noetherian scheme. Let $f : X \to S$ be a proper, flat, surjective morphism such that all its geometric fibers are connected and reduced. Then the natural map $\mathcal{O}_S \to f_*\mathcal{O}_X$ is an isomorphism.

**Proof.** Since $X$ is flat over $S$, $\mathcal{O}_X$ is flat over $S$. Now for each $s \in S$ the natural map

$$(f_*\mathcal{O}_X) \otimes_{\mathcal{O}_S} k(s) \to \mathcal{H}^0(X_s, \mathcal{O}_{X_s})$$

is surjective since it is non-zero (as $1 \mapsto 1$) and the right hand side is 1-dimensional. Thus $\mathcal{O}_X$ satisfies the assumptions in Theorem 10.2.1 (2). We conclude that $f_*\mathcal{O}_X$ is a vector bundle and its formation commutes with base change. Now since $\mathcal{O}_S \to f_*\mathcal{O}_X$ is a map between vector bundles, in order to check that it is an isomorphism it suffices to check that the induced maps $\mathcal{O}_S \otimes_{\mathcal{O}_S} k(s) \to (f_*\mathcal{O}_X) \otimes_{\mathcal{O}_S} k(s)$ are isomorphisms, for all $s \in S$. But the two sides are 1-dimensional $k(s)$-vector spaces and the map is non-zero, so it is an isomorphism. \hfill \Box

11.2. Riemann–Roch for a relative elliptic curve. Let $S$ be a locally noetherian scheme, and $f : E \to S$ an elliptic curve with identity section $e$. Recall that this means that $f$ is a proper smooth morphism with all geometric fibers being connected smooth projective curves of genus 1, and $e : S \to E$ is a distinguished section of $f$. Recall from before that for every positive integer $n$ we have a line bundle $\mathcal{O}(ne)$ on $E$, as well as a map of $\mathcal{O}_S$-modules $\text{Lead}_n : f_*\mathcal{O}(ne) \to e^*(\Omega_{E/S})^\otimes -n$.

**Theorem 11.2.1.** Let $n$ be a positive integer. The following statements hold.

1. For each $s \in S$, $\mathcal{H}^1(E_s, \mathcal{O}(ne)|_{E_s}) = 0$, and $\mathcal{H}^0(E_s, \mathcal{O}(ne)|_{E_s})$ has dimension $n$ over $k(s)$.

2. The $\mathcal{O}_S$-module $f_*\mathcal{O}(ne)$ is a vector bundle of rank $n$, and its formation commutes with arbitrary base change.

3. The composition of the natural maps of $\mathcal{O}_S$-modules $\mathcal{O}_S \to f_*\mathcal{O}_X \to f_*\mathcal{O}(e)$ is an isomorphism.

4. The natural complex of $\mathcal{O}_S$-modules

$$0 \to f_*\mathcal{O}(ne) \to f_*\mathcal{O}((n+1)e) \xrightarrow{\text{Lead}_n} e^*(\Omega_{E/S})^\otimes -n \to 0$$

is exact.

**Proof.** (1) Note that $\mathcal{O}(ne)|_{E_s} = \mathcal{O}_{E_s}(ne_s)$, where $e_s$ is the identity section of the elliptic curve $E_s$ over $k(s)$. Hence the statement follows from the following special case of Riemann–Roch: Let $X$ be a smooth projective curve over a field $k$ (not necessarily algebraically closed) that is geometrically connected and has genus $g$. Let $P \in X(k)$. Then for all $n > 2g - 2$, we have $\mathcal{H}^1(X, \mathcal{O}_X(nP)) = 0$ and $\dim_k \mathcal{H}^0(X, \mathcal{O}_X(nP)) = 1 - g + n$.

(2) This follows from part (1) and Theorem 10.2.1 (1). (Here, since $\mathcal{O}(ne)$ is a line bundle on $E$ and since $E$ is flat over $S$, we know that $\mathcal{O}(ne)$ is indeed flat over $S$.)

(3) Both $\mathcal{O}_S$ and $f_*\mathcal{O}(e)$ are vector bundles whose formation commutes with base change. Thus we reduce to the case where $S$ is the spectrum of a field. Then the statement is classical.

(4) Note the following (easy) fact: Suppose $R$ is a local ring with residue field $k$, and $0 \to A \to B \to C \to 0$ is a complex of finite free $R$-modules. Then this complex is exact if and only if $0 \to A \otimes k \to B \otimes k \to C \otimes k \to 0$ is exact.
Now all three terms in the complex in question are vector bundles over $S$, by part (2) and by the fact that $\Omega_{E/S}$ is a line bundle on $E$. Using the above paragraph, we see that we only need to check that the complex in question becomes exact after $\otimes_{\mathcal{O}_S} k(s)$ for each $s \in S$. But the formation of the three terms commutes with base change (by part (2), and by the functoriality of $\Omega_{E/S}$). Hence we reduce to the case where $S$ is the spectrum of a field. Then the assertion follows from the description of $\text{Lead}_{n+1}$ as taking the $-(n+1)$-th coefficient of the Laurent expansion after choosing a local coordinate around $e$.

11.3. **Local Weierstrass coordinates.** Keep the above notation. After shrinking $S$ around an arbitrary point, we may assume that $S = \text{Spec } R$ and that the line bundle $e^*\Omega_{E/S}$ on $S$ is trivial. Fix a trivialization $e^*\Omega_{E/S}^{\otimes -1} \xrightarrow{\sim} \mathcal{O}_S$, or in other words a basis $\omega$ of the rank 1 free $R$-module $e^*\Omega_{E/S}^{\otimes -1}(S)$. Then for each positive integer $n$, we have a basis $\omega^n$ for the rank 1 free $R$-module $e^*\Omega_{E/S}^{\otimes -n}(S)$. Write $H(n)$ for the $R$-module $(f, \mathcal{O}(n\epsilon))(S)$. We have a short exact sequence of $R$-modules

$$0 \to H(n) \to H(n+1) \xrightarrow{\text{Lead}_{n+1}} R\omega^{n+1} \to 0.$$ 

Now $H(1)$ is canonically identified with $\mathcal{O}_S(S) = R$ (see Theorem 11.2.1 (3)), and $R\omega^{n+1}$ is always free of rank 1. Thus by induction we know that $H(n)$ is a free $R$-module of rank $n$ for each $n \geq 1$. Moreover, the basis $\{1\}$ of $H(1) = R$ can be extended to a basis $\{1, x\}$ of $H(2)$ with

$$\text{Lead}_2(x) = \omega^2,$$

and this can be further extended to a basis $\{1, x, y\}$ of $H(3)$ with

$$\text{Lead}_3(y) = \omega^3.$$

Now using that $\text{Lead}_4(x^2) = \omega^4$, we see that $\{1, x, y, x^2\}$ is a basis of $H(4)$. Similarly, $\{1, x, y, x^2, xy\}$ is a basis of $H(5)$ since $\text{Lead}_5(xy) = \omega^5$; and $\{1, x, y, x^2, xy, x^3\}$ is a basis of $H(6)$ since $\text{Lead}_6(x^3) = \omega^6$. Now $y^2 \in H(6)$, so

$$y^2 = Ax^3 - a_1 xy + a_2 x^2 - a_3 y + a_4 x + a_6$$

for unique $A, a_1, a_2, a_3, a_4, a_6 \in R$. Comparing $\text{Lead}_6$ of both sides we see that $A = 1$. Thus we conclude that $x$ and $y$ satisfy the Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

for unique $a_i \in R$.

12. **Lecture 12**

12.1. **Local Weierstrass coordinates, continued.** We have found a basis $\{1, x\}$ of $H(2) = f_*(\mathcal{O}(2\epsilon))(S)$ and a basis $\{1, x, y\}$ of $H(3) = f_*(\mathcal{O}(3\epsilon))(S)$ such that $\text{Lead}_2(x) = \omega^2$ and $\text{Lead}_3(y) = \omega^3$. We showed that $x$ and $y$ satisfy the Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

for unique $a_i \in R$. We shall call such $x$ and $y$ a choice of **Weierstrass coordinates**.

Now let $\mathcal{W}$ be the closed subscheme of $\mathbb{P}_S^2 = \mathbb{P}_S^2$ defined by the (homogenization of the) above equation (with point at infinity $(0 : 1 : 0)$). Then the $S$-morphism $E \to \mathbb{P}_S^2$ defined by the basis $(x, y, 1)$ of $H(3)$ factors through an $S$-morphism

$$\phi : E \longrightarrow \mathcal{W}.$$
We claim that $\phi$ is an isomorphism. For this, we use the fibral criterion for isomorphism:

Fact: Let $X, Y$ be two $S$-schemes that are locally of finite type and flat over $S$. Let $\phi : X \to Y$ be an $S$-morphism that is of finite type and separated. Then $\phi$ is an isomorphism if and only if $\phi_s : X_s \to Y_s$ is an isomorphism for each $s \in S$.

In order to apply this criterion to $\phi : E \to W$, we need to know that $W$ is flat over $S$, but this follows from the general fact that any hypersurface in $\mathbb{P}_R^n$ defined by a single homogeneous equation whose coefficients generate the unit ideal is flat over Spec $R$. It is also not hard to check that $\phi : E \to W$ is of finite type and separated. Thus we reduce to checking that $\phi_s : E_s \to W_s$ is an isomorphism for all $s \in S$. But the formation of $\phi$ commutes with base change, so we reduce to the case where $S$ is the spectrum of a field. Then the claim is classical; see [Sil09, §III, Prop. 3.1].

Remark. It follows from our claim that $W$ is smooth over $S$. In particular, the discriminant $\Delta$ of the Weierstrass equation (which is a universal polynomial in the variables $a_i$ with integer coefficients, and homogeneous of degree 12 if $a_i$ is assigned weight $i$; see [Sil09, §III.1]) is non-zero in $k(s)$ for all $s \in S^0$, and therefore $\Delta \in R^\times$.

Now let us analyze the uniqueness of the Weierstrass coordinates $x, y$. If we fix the basis $\omega$ of $e^*(\Omega_{E/S})^{\otimes -1}(S)$ fixed, then $x$ and $y$ are unique up to the transformation

$$
\begin{align*}
x & \mapsto x + a \\
y & \mapsto y + bx + c.
\end{align*}
$$

by the defining properties of $x$ and $y$. On the other hand $\omega$ is unique up to $\omega \mapsto u\omega$ for $u \in R^\times$, and this can be matched by the transformation

$$
\begin{align*}
x & \mapsto u^2x \\
y & \mapsto u^3y.
\end{align*}
$$

Thus the group of all admissible transformations is generated by the above two types of transformations. One sees that a general transformation is of the form

$$
\begin{align*}
x & \mapsto u^2x + a \\
y & \mapsto u^3y + u^2bx + c.
\end{align*}
$$

for $a, b, c \in R$ and $u \in R^\times$.

Thus we have shown that given any elliptic curve $E/S$, locally on $S$ we can identify $E$ with the planar curve defined by a Weierstrass equation, and moreover the identification is unique up to the effect of the above transformation group. We might imagine that the “moduli space of elliptic curves” should be given by “Spec $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ modulo the action of the transformation group”. Unfortunately this does not work in the category of schemes. In the next few lectures, we will show that a level-3 structure can help to rigidify the Weierstrass equation to the extent that none of the above transformations are allowed. Then we will be able to prove the representability of $S(3)$.

---

5This is because over a field, a Weierstrass equation defines a non-singular curve if and only if $\Delta \neq 0$. In fact, in the classical proof ([Sil09, §III, Prop. 3.1]) that our $\phi : E \to W$ is an isomorphism when $S$ is the spectrum of a field, it is shown a priori that the Weierstrass equation must be non-singular.
13. Lecture 13

13.1. Construction of \( S(3) \). As before, let \( f : E \to S \) be an elliptic curve, with identity section \( e : S \to E \). Recall that if \( S = \text{Spec} \, R \) and \( e^*E_{\ell}/S \cong O_S \), then we can find Weierstrass coordinates \( x \) and \( y \) on \( E \) such that \( E \) is the relative curve in \( \mathbb{P}^2_S \) defined by

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6
\]

for unique \( a_i \in R \). Here \( e \) corresponds to the homogeneous coordinate \((0 : 1 : 0)\). Moreover, the \( x \) and \( y \) are unique up to transformation

\[
\begin{align*}
x' &= u^2x + a \\
y' &= u^3y + bu^2x + c
\end{align*}
\]

\( a, b, c \in R, \quad u \in R^\times \).

We will explain how to use a full level-3 structure to rigidify the situation, which will eventually lead to the construction of the moduli space \( S(3) \). Our explanation will be informal to begin with.

Suppose \( S = \text{Spec} \, k \) where \( k \) is a field with char \( k \neq 3 \). Let \((P, Q)\) be a level 3 structure, namely, \( P, Q \in E[3](k) \) such that they form an \( \mathbb{F}_3 \)-basis of

\[ E[3](k) \cong \mathbb{F}_3. \]

Note in particular that this implies that \( E[3](k) = E[3](\bar{k}) \). Then we take Weierstrass coordinates \( x \) and \( y \) in the classical sense such that \( E \) is defined by \( y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \) where \( a_i \in k \).

Now, the fact that \( 3P = e \) implies that \( 3[P] - 3[e] \) is a principal divisor, i.e., there exists \( \varphi \in k(E) \) such that \( \text{div}(\varphi) = 3[P] - 3[e] \). Note that we have \( \varphi \in H(3) \setminus H(2) \) where \( H(n) := (f,\cO(ne))(k) = H^0(E,\cO(ne)) \). We may assume that \( \text{Lead}_3(\varphi) = \omega^3 \) where \( \omega \) is the fixed basis of \( e^*O_{E/S}^\times \). Hence we could have chosen \( y \) to be \( \varphi \). Namely, we may assume \( \text{div}(y) = 3[P] - 3[e] \). So we have \( y(P) = 0 \). Now \( x(P) \) may not be zero, but we can always replace \( x \) by \( x - x(P) \). In summary, we may assume \( P = (0,0) \).

Next we discuss negation on \( E \). Take \( T \in E(k) \). By the definition of the group law, the three points \( T, -T \), and the “point at infinity” \( e = (0 : 1 : 0) \in \mathbb{P}^2(k) \) are colinear. Thus the \( x \)-coordinate of \(-T\) is the same as that of \( T \). Now if \( y_1, y_2 \) are the two roots of the equation

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6
\]

for some fixed \( x_0 \), then \( y_1 + y_2 = -(a_1x_0 + a_3) \) by Vieta theorem. Hence if \( T \) has coordinate \((x, y)\) then \(-T\) has coordinate \((x, -y - a_1x - a_3)\). Now applying this to \( P = (0, 0) \), we get \(-P = (0, -a_3)\). Since \(-P \neq P \) (as \( P \) is a non-trivial 3-torsion point), we have \( a_3 \neq 0 \).

Now recall that \( x \in H(2) \setminus H(1) \), which means that the only pole that \( x \) has is a pole of order 2 at \( e \). We have seen that both \( P \) and \(-P\) has zero \( y \)-coordinate, so \( x \) has at least a zero at \( P \) and at least a zero at \(-P\). Therefore \( \text{div}(x) = [P] + [-P] - 2[e] \). Now recall that \( \text{div}(y) = 3[P] - 3[e] \). From here, we see that

\[ \text{ord}_P(y^2 + a_1xy + a_3y) \geq 3. \]

We also see that \( \text{ord}_P(x^3) = 3 \). Hence \( \text{ord}_P(a_2x^2 + a_4x + a_6) \geq 3 \). But we know that \( \text{ord}_P(x) = 1 \). This implies that \( a_2 = a_4 = a_6 = 0 \). Therefore the Weierstrass equation is forced to be of the form

\[ y^2 + a_1xy + a_3y = x^3 \]
where \( a_3 \neq 0 \) and \( \Delta \neq 0 \). Here \( \Delta \) is the discriminant \( \Delta = \Delta(a_1,a_3) = a_1^3 a_3^3 - 27 a_4^4 \) (see [Sil09, §III.1]). Note that the only allowed transformations of coordinates are

\[
\begin{align*}
  y' &= u^3 y \\
  x' &= u^2 x
\end{align*}
\]

by easy considerations on the vanishing orders of \( x \) and \( y \) at \( P \).

Now, we consider \( Q \). There exists unique \( A, B \in k \) such that

\[
\text{div}(y - Ax - B) = 3[Q] - 3[e]
\]

because the right hand side is a principal divisor and has exactly a pole of order 3 at \( e \).

Now, we consider the system of equations

\[
\begin{align*}
  y &= Ax + B \\
  y^2 + a_1 x y + a_3 y &= x^3
\end{align*}
\]

After substituting the first equation into the second equation, we obtain

\[
x^3 - (Ax + B)^2 - a_1 x(Ax + B) - a_3(Ax + B) = 0.
\]

The fact that \( y - Ax - B \) has a triple zero at \( Q \) precisely means that the above equation has a triple zero at \( x = x(Q) \). Hence we have

\[
x^3 - (Ax + B)^2 - a_1 x(Ax + B) - a_3(Ax + B) = (x - x(Q))^3.
\]

By comparing coefficients, we will see that \( a_1, a_3 \) are related to \( A \) and \( B \).

14. Lecture 14

14.1. Construction of \( S(3) \), continued. Recall our setup from before. Fix an elliptic curve \( E \) over a field \( k \) with \( \text{char } k \neq 3 \). We also fix a level-3 structure \((P, Q)\). By choosing Weierstrass coordinates \( x \) and \( y \) such that \( P = (0,0) \) and \( \text{div}(y) = 3[Q] - 3[e] \), we can deduce that the Weierstrass equation is of the form

\[
y^2 + a_1 x y + a_3 y = x^3.
\]

We also know that the discriminant \( \Delta = \Delta(a_1,a_3) \) \(:= a_1^3 a_3^3 - 27 a_4^4 \) is non-zero, which implicitly implies \( a_3 \neq 0 \).

Now we consider \( Q \). Since \( Q \) is also 3-torsion and \( Q \neq e \), we know that \( 3[Q] - 3[e] \) is principal divisor. Hence we can find unique \( A, B \in k \) such that \( \text{div}(y - Ax - B) = 3[Q] - 3[e] \).

The fact that \( y - Ax - B \) has a triple zero at \( Q \) precisely means the following identity

\[
(14.1) \quad x^3 - (Ax + B)^2 - a_1 x(Ax + B) - a_3(Ax + B) = (x - x(Q))^3.
\]

Note that different powers of \( x \) are linearly independent over \( k \), so we can compare coefficients in \((14.1)\) to get relations among \( a_1, a_3, A, B \). In particular, for the quadratic coefficient, we see \(-A^2 - a_1 A = -3x(Q)\). Note also that \( Q \neq \pm P \) since \((P, Q)\) is a level 3 structure. This implies \( x(Q) \neq 0 \). So we have \( A \neq 0 \). Then by the change of coordinates

\[
\begin{align*}
  x &\mapsto A^2 x \\
y &\mapsto A^3 y
\end{align*}
\]

we may assume that \( A = 1 \).
Now set $x(Q) =: C \neq 0$. Since $y - x - B$ vanishes at $Q$, we have $y(Q) = B + C$, i.e., $Q = (C, B + C)$. Comparing coefficients in (14.1) we get

$$\begin{cases}
    a_1 = 3C - 1, \\
    a_3 = -3C^2 - B - 3BC, \\
    B^3 = (B + C)^3.
\end{cases}$$

Using the above, we think of $\Delta = \Delta(a_1, a_3)$ as a polynomial in $B, C$. In order to avoid conflict of notation we denote this polynomial by $\Delta_{B,C} \in \mathbb{Z}[B, C]$.

In conclusion, starting with $(E, P, Q)$, we can choose Weierstrass coordinates $x$ and $y$ on $E$ such that $P = (0, 0)$ and $Q = (C, B + C)$, and such that the Weierstrass equation (uniquely determined after choosing $x$ and $y$) is of the form

$$y^2 + a_1 xy + a_3 y = x^3$$

where

$$\begin{cases}
    a_1 = 3C - 1, \\
    a_3 = -3C^2 - B - 3BC.
\end{cases}$$

Moreover, $B, C \in k$ satisfy

$$\begin{cases}
    C \neq 0, \\
    \Delta_{B,C} \neq 0, \\
    B^3 = (B + C)^3.
\end{cases}$$

(Recall that $C \neq 0$ comes from the condition $Q \not\in \{\pm P, e\}$, and from $\Delta_{B,C} \neq 0$ we have $a_3 \neq 0$ which corresponds to $P \not\in \{-P, e\}$.)

Conversely, suppose we start with $B, C \in k$ satisfying the conditions (14.2). We set $a_1 := 3C - 1$ and $a_3 := -3C^2 - B - 3BC$, and then define

$$\begin{aligned}
    E_{B,C} &:= \{y^2 + a_1 xy + a_3 y = x^3\} \subset \mathbb{P}^2_k, \\
    P_{B,C} &:= (0, 0), \\
    Q_{B,C} &:= (C, B + C).
\end{aligned}$$

Then $E_{B,C}$ is an elliptic curve over $k$ and $(P_{B,C}, Q_{B,C})$ is a level-3 structure for $E_{B,C}$.

Also, for any given $(E, P, Q)$, there is a unique choice of Weierstrass coordinates $x$ and $y$ rendering $(E, P, Q)$ in the above standard form for unspecified $B, C$. Indeed, if $x$ and $y$ render $(E, P, Q)$ in the standard form, then we can show that

$$\begin{aligned}
    \text{div}(y) &= 3[P] - 3[e], \\
    \text{div}(x) &= |P| + |-P| - 2[e], \\
    \text{div}(y - x - B) &= 3|Q| - 3[e].
\end{aligned}$$

It is then easy to see that there is no non-trivial coordinate change

$$\begin{cases}
    x' = u^2 x + a \\
    y' = u^3 y + bu^2 x + c
\end{cases}, \quad a, b, c \in k, \quad u \in k^\times$$

preserving these three conditions.

This uniqueness means that for any $(E, P, Q)$, there exist unique $B, C$ and a unique isomorphism $(E, P, Q) \xrightarrow{\sim} (E_{B,C}, P_{B,C}, Q_{B,C})$.

Now imagine that we may perform this construction in the relatively setting, i.e., we can show that for all elliptic curves $E/S$ where $S$ is defined over $\mathbb{Z}[1/3]$, after localizing $S$
(i.e., passing to a Zariski open covering), there exist unique Weierstrass coordinates \( x \) and \( y \) rendering \( (E, P, Q) \) in the standard form as above. In particular, by uniqueness, we see that passing to a Zariski open covering of \( S \) is not necessary, because the local Weierstrass coordinates and the local sections \( B, C \) must be compatible on the overlaps of the open covering. Thus, for all locally noetherian \( S/\mathbb{Z}[1/3] \) (not necessarily affine) and any \( E/S \) with level-3 structure \( (P, Q) \), there exist unique \( B, C \in \mathcal{O}_S(S) \) and a unique isomorphism from \( (E, P, Q) \) to the standard \( (E_{B,C}, P_{B,C}, Q_{B,C}) \) inside \( \mathbb{P}^2_S \). We may state this even more precisely as follows.

**Theorem 14.1.1.** The functor

\[
S(3): \{\text{locally noetherian schemes over } \mathbb{Z}[1/3]\} \rightarrow (\text{Sets})
\]

sending \( S \) to the set of isomorphism classes of elliptic curves \( E/S \) with level-3 structure \( (P, Q) \), is represented by the \( \mathbb{Z}[1/3] \)-scheme

\[
\text{Spec } \mathbb{Z}[1/3, B, C, C^{-1}, \Delta_{B,C}^{-1}]/(B^3 - (B + C)^3).
\]

The universal object is given by \((E_{B,C}, P_{B,C}, Q_{B,C})\).

The proof roughly follows the same ideas as our discussion over a field. For the complete rigorous proof, see [Conc., §4]. There are two interesting points in the proof which we intend to elaborate on:

1. Assume \( S = \text{Spec } R \) and \( e^* \Omega_{E/S} \) is trivial, so Weierstrass coordinates exist. Up to further shrinking \( S \), for any fixed Weierstrass coordinates \( x \) and \( y \), there are unique \( a, b \in R \) such that the suitable analog of the statement \( \text{div}(y + ax + b) = 3[P] - 3[e] \) holds. Thus we can replace \( y \) by \( y + ax + b \).

2. In the same setting as (1), the morphism \([-1]: E \rightarrow E \) is still given by \((x : y : z) \mapsto (x : y - a_1x - a_3 : z)\), as in the case over a field.

15. Lecture 15

15.1. **Construction of \( S(3) \), technical details.** Recall that last lecture, we informally showed that the functor

\[
S(3): \{\text{locally noetherian schemes over } \mathbb{Z}[1/3]\} \rightarrow (\text{Sets})
\]

sending \( S \) to the set of isomorphism classes of elliptic curves \( E/S \) with level-3 structure \( (P, Q) \), is represented by the \( \mathbb{Z}[1/3] \)-scheme

\[
\text{Spec } \mathbb{Z}[1/3, B, C, C^{-1}, \Delta_{B,C}^{-1}]/(B^3 - (B + C)^3).
\]

The universal object is given by \((E_{B,C}, P_{B,C}, Q_{B,C})\).

**Remark.** The scheme \( S(3) \) is affine and smooth over \( \mathbb{Z}[1/3] \), with fibers of pure dimension 1.

We now elaborate on the two technical details stated at the end of last lecture. In this lecture we discuss (1). Suppose we have Weierstrass coordinates \( x, y \), adapted to the choice of an \( R \)-basis \( \omega \) of \( e^*(\Omega_{E/S})^\otimes-1(S) \) (so \( \text{Lead}_2(x) = \omega^2 \) and \( \text{Lead}_3(y) = \omega^3 \)). Recall that for each \( p \in E(S) \), we have the ideal sheaf for the closed subscheme \( p(S) \subset E \), denoted \( I_p \subset \mathcal{O}_E \). This is an invertible \( \mathcal{O}_E \)-module, and we have the notation \( \mathcal{O}(np) := T_p^\otimes-n \). Recall that \( \{1, x\} \) is an \( R \)-basis of \((f^* \mathcal{O}(2e))(S) = \mathcal{O}(2e)(E) = I_p^\otimes-2(E) \) such that \( \text{Lead}_2(x) = \omega^2 \) where

\[
\text{Lead}_2 : (f^* \mathcal{O}(2e))(S) \rightarrow (e^* \Omega_{E/S})^\otimes-2(S) \cong R \cdot \omega^2.
\]
Also, \( \{1, x, y\} \) is an \( R \)-basis of \( \mathcal{I}_e^{\otimes -3}(E) \) such that \( \text{Lead}_3(y) = \omega^3 \) where
\[
\text{Lead}_3 : \mathcal{I}_e^{\otimes -3}(E) \longrightarrow R \cdot \omega^3.
\]

Note that there is a natural injective map of \( \mathcal{O}_E \)-modules
\[
\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3} \hookrightarrow \mathcal{I}_e^{\otimes -3}
\]
as \( \mathcal{I}_p^{\otimes 3} = \mathcal{I}_p^3 \) is an ideal sheaf of \( \mathcal{O}_E \). So there is a natural \( \mathcal{O}_S \)-module embedding
\[
f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3}) \hookrightarrow f_*(\mathcal{I}_e^{\otimes -3}).
\]
The desired generalization of the statement “\( \exists a, b \) such that \( \text{div}(y + ax + b) = 3[P] - 3[e] \)” which makes sense over a field is the following statement:

- (After further shrinking \( S \) if necessary), \( \exists a, b \in R \) such that the global section \( y + ax + b \) of \( f_*(\mathcal{I}_e^{\otimes -3}) \) generates the \( \mathcal{O}_S \)-submodule \( f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3}) \). (Since \( S \) is affine, this is equivalent to requiring that \( y + ax + b \) is an \( R \)-basis of the \( R \)-submodule \( f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3})(S) \subset f_*(\mathcal{I}_e^{\otimes -3})(S) \). )

We now prove this statement. Recall that the group law on \( E \) is given such that for three points \( p, q, r \in E(S) \) we have \( p + q = r \) if and only if
\[
\mathcal{I}_p \otimes \mathcal{I}_q \otimes \mathcal{I}_e^{\otimes -2} \cong \mathcal{I}_r \otimes \mathcal{I}_e^{\otimes -1} \otimes f^* \mathcal{L}
\]
for some line bundle \( \mathcal{L} \) on \( S \). Since \( P \in E[3] \), we have \( \mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3} \cong f^* \mathcal{L} \) for some line bundle \( \mathcal{L} \) on \( S \). After shrinking \( S \), we may assume that \( \mathcal{L} \) is trivial. In particular, we may ensure that \( \mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3} \cong \mathcal{O}_E \) (non-canonically).

Now recall that since \( E/S \) is proper and flat, with reduced and connected geometric fibers, we know that \( f_*\mathcal{O}_E \cong \mathcal{O}_S \) canonically. So we know that non-canonically, we have
\[
f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3}) \cong \mathcal{O}_S,
\]
i.e., \( f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3}) \) is a (trivial) line bundle on \( S \).

Now consider the composition
\[
\varphi_{E,P} : f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3}) \hookrightarrow f_*(\mathcal{I}_e^{\otimes -3}) \xrightarrow{\text{Lead}_3} e^*(\Omega_{E/S})^{\otimes -3}.
\]
We claim that \( \varphi_{E,P} \) is an isomorphism. Since both the source and target are line bundles, it suffices to check that \( \varphi_{E,P} \) induces isomorphisms on all geometric fibers. For this, note that for each geometric point \( \bar{s} : \text{Spec} \ k \to S \), the map
\[
f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3}) \otimes \mathcal{O}_{E,\bar{s}} \to e^*(\Omega_{E/S})^{\otimes -3} \otimes \mathcal{O}_{E,\bar{s}}
\]
induced by \( \varphi_{E,P} \) is identified with \( \varphi_{E_\bar{s},P_\bar{s}} \), i.e., the same construction but applied to the elliptic curve \( E_\bar{s} \) over \( k \) and the point \( P_\bar{s} \in E_\bar{s}[3](k) \) induced by \( P \). Thus in order to check that \( \varphi_{E,P} \) is an isomorphism, we may assume that \( S = \text{Spec} \ k \) for an algebraically closed field. Then \( \varphi_{E,P} \) becomes, for a choice of a local coordinate \( z \) around \( e \), the map
\[
\varphi_{E,P} : H^0(E, \mathcal{O}(3[P] - 3[e])) \xrightarrow{\text{Lead}_3} k,
\]
sending each function to the coefficient of \( z^{-3} \) in its Laurent expansion near \( e \). Since \( P \in E[3] \), we see that there is a function in the left hand side whose divisor is precisely \( 3[P] - 3[e] \). Hence \( \varphi \) is surjective. Also, we see that \( \varphi^{-1}(0) \) is the set of \( h \in k(E) \) that have at most 2 poles at \( e \), no other poles, and at least 3 zeros at \( P \). But this must just be 0. Hence \( \varphi \) is injective as well. The claim is proved.

By the claim, there is a unique global section of \( f_*(\mathcal{I}_p^{\otimes 3} \otimes \mathcal{I}_e^{\otimes -3}) \) that generates this line bundle and which has image \( \omega^3 \) under \( \text{Lead}_3 \). Then this global section must be of the desired form \( y + ax + b \) for unique \( a, b \in R \).
16. Lecture 16

16.1. The inversion formula and the Rigidity Lemma. Next, we will prove the following fact, which we recall is another key ingredient in the proof of the representability of $S(3)$.

**Proposition 16.1.1.** Let $S = \text{Spec} R$ be an affine scheme, and suppose $E/S$ is an elliptic curve given by the Weierstrass equation $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ in $\mathbb{P}_R^2$ (with identity section $(0 : 1 : 0)$). Then $[-1] : E \to E$ is given by $(x : y : z) \mapsto (x : -y - a_1 x - a_3 : z)$.

Proof. Note that the claimed formula gives an endomorphism of $E$, in the sense that this is an $S$-scheme morphism $E \to E$ preserving the identity section; (this indeed implies that this is a morphism of group schemes, but we will not need this fact). This formula and the abstract morphism $[-1] : E \to E$ are two endomorphisms of $E$ that agree on geometric fibers. We conclude by the following fact. □

**Fact 16.1.2.** If $E/S$ is an elliptic curve and $\varphi, \varphi' : E \to E$ are endomorphisms of elliptic curves (in the above sense) such that they agree on $E_\xi$ for each geometric point $\xi$ of $S$, then $\varphi = \varphi'$.

Remark. In fact the analogous statement is true for general abelian schemes.

This fact following from the following Rigidity Lemma.

**Theorem 16.1.3** (Rigidity Lemma). Suppose $G$ is a group scheme over an arbitrary base scheme $S$. Suppose $f : X \to S$ is a proper (or just closed, which is enough) morphism such that $f_* \mathcal{O}_X \cong \mathcal{O}_S$. Suppose $\varphi, \varphi' : X \to G$ are two $S$-morphisms that agree on each geometric fiber. Then $\varphi$ and $\varphi'$ differ by multiplication (with respect to the group structure of $G$) by a section $\gamma \in G(S)$.

For a proof, see [Conb, §4].

Remark. Recall one sufficient set of conditions for the hypothesis $f_* \mathcal{O}_X \cong \mathcal{O}_S$: when $f$ is proper, flat, and surjective with connected and reduced geometric fibers.

Remark. To see that we need not have $\varphi = \varphi'$, consider the case when $S = \text{Spec} k[\epsilon]/(\epsilon^2)$ for some field $k$, and $G = \mathbb{G}_a/S = \mathbb{A}_k^1$. Set $f : X = S \to S$ to be the identity. Then $S$-maps from $X$ to $G$ form the additive group $G(S) = (k[\epsilon]/(\epsilon^2), +)$. We may set $\varphi = 0$ and $\varphi' = \epsilon$. They indeed agree on geometric fibers.

Proof of Fact 16.1.2. By the Rigidity Lemma, $\varphi$ and $\varphi'$ differ by some $\gamma \in E(S)$. But $\varphi$ and $\varphi'$ both preserve the identity section, and hence $\gamma$ must be trivial. □

16.2. Relative representability of level structures. We have already (informally) proved the representability of $S(3)$ over $\mathbb{Z}[1/3]$ by an affine, smooth scheme over $\mathbb{Z}[1/3]$. We accept the same for $S(4)$ (over $\mathbb{Z}[1/2] = \mathbb{Z}[1/4]$) without proof. Our next objective is to prove the following theorem.

**Theorem 16.2.1.** For $N \geq 3$, the functor

$$S(N) : (\text{Locally noetherian schemes over } \mathbb{Z}[1/N]) \longrightarrow (\text{Sets})$$

given by

$$T \mapsto \{\text{iso. cl. of elliptic curves } E/T \text{ with level-N structure}\}$$

is representable by a smooth affine scheme over $\mathbb{Z}[1/N]$. 

34 YIHANG ZHU
The idea is to consider the forgetful map $S(N) \to S(1)$, where $S(1)$ is the fibered groupoid of elliptic curves (i.e., for each test scheme $S$, $S(1)(S)$ is the groupoid of all elliptic curves over $S$, namely the category of all elliptic curves over $S$ where the only allowed morphisms are isomorphisms; if we have a morphism $S \to S'$, then we have a functor $S(1)(S') \to S(1)(S)$ given by pullback). We want to show that for each $Z$ scheme over $S$, the pullback of $S(N) \to S(1)$ over $S$ along $E \in S(1)(S)$ should be representable by a scheme over $S$. Let us state this more concretely as follows.

**Theorem 17.1.2** (Relative representability of level structures). Let $N \geq 1$. Let $S$ be a scheme over $\mathbb{Z}[1/N]$, and let $E/S$ be an elliptic curve. The functor

$$\text{(schemes over } S) \longrightarrow \text{(Sets)}$$

given by

$$T \mapsto \{\text{level-N structures on } E_T = E \times_S T\}$$

is representable by an $S$-scheme $I_{E/S,N}$. Moreover, $I_{E/S,N}$ is an étale $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$-torsor over $S$ under the natural $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$-action. (See the beginning of the next lecture for étale torsors.)

17. Lecture 17

17.1. Relative representability of level structures, continued. We first briefly recall some terminology. Suppose $G$ is a finite group and $S$ is a scheme. An étale $G$-torsor over $S$ is a scheme $X$ over $S$ which is finite étale and surjective over $S$, together with an action of $G$ on $X$ via $S$-automorphisms such that the map

$$G_S \times_S X \longrightarrow X \times_S X$$

given for all $S$-schemes $T$ via $G \times X(T) \to X(T) \times X(T), (g, x) \mapsto (gx, x)$ is an isomorphisms of $S$-schemes. (Here $G_S$ denotes the constant group scheme over $S$ given by $G$.) Equivalently, since $X$ is finite étale and surjective over $S$, the condition on the action of $G$ amounts to imposing that for all geometric points $\text{Spec } \overline{k} \to S$, the action of $G$ on $X(\overline{k})$ is free and transitive.

**Example.** Suppose $k'/k$ is a finite Galois extension of fields. Take $X = \text{Spec } k'$ and $S = \text{Spec } k$. Let $G = \text{Gal}(k'/k)$. Then $X$ is an étale $G$-torsor over $S$. Note that the action of $G$ on $X(k)$ is not free; $X(k)$ has only one element.

We now state and prove the relative representability of $S(N)$ over $S(1)$.

**Theorem 17.1.1** (relative representability of level structures). Let $N$ be a positive integer and $S$ a scheme over $\mathbb{Z}[1/N]$. Fix an elliptic curve $E/S$. The functor

$$\text{(S-schemes) } \longrightarrow \text{(Sets)}$$

given by

$$T \mapsto \{\text{level-N structures on } E_T = E \times_S T, \ i.e., \ isomorphisms } \gamma : (\mathbb{Z}/N\mathbb{Z})^2_T \sim \to E_T[N]\}$$

is representable by a scheme $I_{E/S,N}$ which is an étale $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$-torsor over $S$.

**Proof.** We will use the following two facts, which we admit.

1. Since $S$ is over $\mathbb{Z}[1/N]$, the group scheme $E[N]$ is finite étale over $S$.
2. For any $S$-scheme $T$, we have a canonical identification $E_T[N] \cong E[N] \times_S T$. 

SHIMURA VARIETIES 35
We define an $S$-scheme

$$M := E[N] \times_S E[N] = \{(P, Q) \mid P, Q \in E[N]\}.$$

We have a universal homomorphism

$$h : \left(\mathbb{Z}/N\mathbb{Z}\right)^2_M \to E_M[N] = E[N] \times_S M$$

given by

$$h(i, j) = iP + jQ, \quad \forall i, j \in \mathbb{Z}/N\mathbb{Z},$$

where $(P, Q)$ is the “universal element of $E[N] \times E[N]$”, i.e., the section of

$$E_M[N] \times_M E_M[N] = E[N] \times_S E[N] \times_S M = M \times M \to M$$

given by the diagonal $M \to M \times_M M$. Abstractly, the functor

$$(S\text{-schemes}) \to (\text{Sets}), \quad T \mapsto \{\text{homomorphisms } \left(\mathbb{Z}/N\mathbb{Z}\right)^2_T \to E_T[N]\}$$

is represented by the $S$-scheme $M$, and $h$ is the universal object.

We want to construct $I_{E/S,N}$ as a suitable locus in $M$ over which $h$ is an isomorphism. This can indeed be done by throwing away certain connected components of $M$. More precisely, notice that for each connected component $M_i$ of $M$, exactly one of the following must be true.

1. $h|_{M_i} : \left(\mathbb{Z}/N\mathbb{Z}\right)^2_{M_i} \to E_{M_i}[N]$ is an isomorphism.

2. For each geometric point $x : \text{Spec} \bar{k} \to M_i$, the homomorphism $h_x : \left(\mathbb{Z}/N\mathbb{Z}\right)^2_x \to E_x[N]$ is not an isomorphism.

Indeed, for each geometric point $x : \text{Spec} \bar{k} \to M_i$, we have the following equivalence of categories:

$$(\text{finite étale } M_i\text{-schemes}) \to (\text{finite } \pi_1^\text{ét}(M_i, x)\text{-sets}), \quad Y \mapsto Y_x(\bar{k}).$$

This follows from Grothendieck’s Galois theory for schemes and the fact that $M_i$ is connected. Now both the source and target of $h|_{M_i}$ are finite étale $M_i$-schemes. If $h_x$ is an isomorphism, then the image of $h|_{M_i}$ under the above equivalence of categories is an isomorphism between $\pi_1^\text{ét}(M_i, x)$-sets (since it is a bijection of sets and equivariant under $\pi_1^\text{ét}(M_i, x)$). This implies that $h_{M_i}$ is an isomorphism.

Now notice that for any $S$-scheme $T$ and any isomorphism $\gamma : \left(\mathbb{Z}/N\mathbb{Z}\right)^2_T \to E_T[N]$, the resulting $S$-scheme morphism $T \to M$ arising from $\gamma$ will factor through the union $U$ of those connected components $M_i$ satisfying (1) above, because otherwise there will be a geometric point of $T$ over which $\gamma$ is not an isomorphism. Conversely, if we have an $S$-scheme morphism $T \to U \subset M$, then the pullback of $h$ to $T$ is an isomorphism. In particular, this indicates that the functor in the theorem is represented by $I_{E/S,N} := U$.

Since $M$ is finite étale over $S$, we know that $I_{E/S,N}$ is finite étale as well. Also, using the moduli interpresentation of $I_{E/S,N}$, we can easily see that $I_{E/S,N} \to S$ is surjective and a $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$-torsor.

### 17.2. Back to the construction of the modular curve.

We now have enough to start proving the representability of $S(N)$.

**Theorem 17.2.1.** Let $N \geq 3$. The functor

$$S(N) : (\text{locally noetherian schemes over } \mathbb{Z}[1/N]) \to (\text{Sets})$$

given by

$$S \mapsto \{\text{iso. cl. of elliptic curves over } S \text{ with level-}N \text{ structure}\}$$
is representable by a smooth affine scheme over \( \mathbb{Z}[1/N] \) with all fibers pure of dimension 1.

Proof. We assume this for \( N = 3 \) and \( N = 4 \). Suppose that \( N \geq 5 \) is general. We proceed along cases.

**Case (a):** Suppose \( 3|N \). We have an open immersion \( \text{Spec} \mathbb{Z}[1/N] \subset \text{Spec} \mathbb{Z}[1/3] \). We have already constructed \( S(3) \) as a moduli scheme over \( \mathbb{Z}[1/3] \). We denote the universal object over \( S(3) \) as \((E_3, \gamma_3)\). We write \( S(3)[\frac{1}{N}] \) for the base change of \( S(3) \) over \( \mathbb{Z}[1/N] \). Then we obtain \( S(N) \) by the following fiber product:

\[
S(N) \longrightarrow I_{E_3/S(3)[\frac{1}{N}]}, \quad \gamma_3 \downarrow \text{forget} \quad \downarrow \quad I_{E_3/S(3)[\frac{1}{N}]}, \gamma_3
\]

Here, the right vertical map is defined by the canonical process of obtaining a level 3-structure from a level \( N \)-structure, namely by identifying \((\mathbb{Z}/3\mathbb{Z})^2 \) (resp. \( E[3] \)) with the 3-torsion inside \((\mathbb{Z}/N\mathbb{Z})^2 \) (resp. \( E[N] \)). This map is finite étale. Hence \( S(N) \) if finite étale over \( S(3)[1/N] \), and therefore it is smooth, affine, of pure relative dimension 1 over \( \mathbb{Z}[1/N] \) as \( S(3)[1/N] \) has the same properties.

**Case (b):** Suppose \( 4|N \). Then we proceed as in Case (a), making use of \( S(4) \) instead of \( S(3) \).

In the next lecture, we will treat the case when neither 3 or 4 divides \( N \). \( \square \)

18. Lecture 18

18.1. The construction of the modular curve, continued.

**Proof of Theorem 17.2.1, continued.** In the last lecture we constructed \( S(N) \), in the case where 3 or 4 divides \( N \), by taking a fiber product. That the fiber product indeed represents the correct functor follows from statement (1) in Lemma 18.1.1 below.

**Case (c):** Suppose \( N \) is coprime to 6. We have an open covering

\[ \{\text{Spec} \mathbb{Z}[1/2N], \text{Spec} \mathbb{Z}[1/3N]\} \]

of \( \text{Spec} \mathbb{Z}[1/N] \). It suffices to construct \( S(N) \) over \( \mathbb{Z}[1/2N] \) and over \( \mathbb{Z}[1/3N] \) separately, because over \( \text{Spec} \mathbb{Z}[1/2N] \cap \text{Spec} \mathbb{Z}[1/3N] \) the two constructions must be canonically isomorphic by Yoneda’s lemma, which allows us to glue the two constructions together to obtain \( S(N) \) over \( \mathbb{Z}[1/N] \).

We construct \( S(N) \) over \( \mathbb{Z}[1/3N] \). We already have \( S(3N) \) over \( \mathbb{Z}[1/3N] \) by Case (a). Let \( K = \ker(\text{GL}_2(\mathbb{Z}/3N\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})) \). The group \( \text{GL}_2(\mathbb{Z}/3N\mathbb{Z}) \), and therefore \( K \), acts on \( S(3N) \) via the moduli interpretation of \( S(3N) \) by permuting the level-3N structure, i.e.,

\[ g \cdot (E, \gamma) = (E, \gamma \circ g^{-1}), \quad \forall (E, \gamma) \in S(N)(S), \forall \text{ loc. noeth. } \mathbb{Z}[1/3N]-\text{scheme } S. \]

Now for any locally noetherian \( \mathbb{Z}[1/3N]-\text{scheme } S \) and any elliptic curve \( E/S \), after étale localization on \( S \), to give a level \( N \)-structure on \( E/S \) is the same as to give a \( K \)-orbit of level-3N structures. (The étale localization on \( S \) is needed just to guarantee the existence of one level 3N-structure on \( E \); for instance we can use the finite étale cover \( I_{E/S,3N} \to S \) to achieve this.) This suggests that the \( K \)-action should make \( S(3N) \) an étale \( K \)-torsor over \( S(N)[\mathbb{Z}[1/3N]] \) (which is yet to be constructed). In turn, we should construct \( S(N)[\mathbb{Z}[1/3N]] \) as
the quotient of $S(3N)$ by $K$. This quotient is of the simplest type in algebraic geometry as we now explain.

Suppose $X \to Y$ is a morphism of finite type between affine schemes $X = \text{Spec} B$ and $Y = \text{Spec} A$. Assume that $Y$ is noetherian. Let $G$ be a finite group acting on $X$ via $Y$-scheme automorphisms. Suppose for any geometric point $\text{Spec} k \to Y$, the action of $G$ on $X(k) = \{Y$-morphisms $\text{Spec} k \to X\}$ is free. Then $X/G := \text{Spec}(B^G)$ is again a $Y$-scheme of finite type, and the natural map $X \to X/G$ is an étale $G$-torsor. Moreover, $X/G$ is the categorical quotient of $X$ by $G$, in the sense that for every $Y$-scheme $Z$, every $G$-invariant $Y$-scheme map $X \to Z$ factors uniquely through $X \to X/G$. Furthermore, $X/G$ is the geometric quotient of $X$ by $G$ in the sense that the topological space $|X/G|$ is the quotient space of $|X|$ by $G$. The reference for these statements is [Gro03, V, §1, §2]. (See also [Mum08, §6] when the base is an algebraically closed field.)

Now in our case, the $K$-action on the $\mathbb{Z}[1/3N]$-scheme $S(3N)$ satisfies the freeness hypothesis in the above paragraph, by statement (1) in Lemma 18.1.1 below. (For each geometric point $\text{Spec} k \to \text{Spec} \mathbb{Z}[1/3N]$, each $K$-orbit in $S(3N)(k)$ is equal to the set on the right hand side of the bijection in Lemma 18.1.1 (1) for some choice of $(E, \gamma)$ (with $N' = 3N$). But clearly the $K$-action on the left hand side is free.) Hence we can form the quotient $S(3N)_{\mathbb{Z}[1/3N]} := S(3N)/K$, and $S(3N) \to S(N)_{\mathbb{Z}[1/3N]}$ is an étale $K$-torsor.

We now give a rigorous argument justifying that $S(N)_{\mathbb{Z}[1/3N]}$ constructed above indeed represents the correct functor. To simplify notation we write $\mathcal{S} = S(N)_{\mathbb{Z}[1/3N]}$. We will use the assumption that $N$ is coprime to 3 in order to simplify the argument, although this could be avoided without too much difficulty. Firstly, we need to construct a universal object over $\mathcal{S}$. Over $S(3N)$ we have the universal object $(E_{3N}, \gamma_{3N})$, and we let $\gamma'_{3N}$ be the level-$N$ structure on $E_{3N}$ induced by $\gamma_{3N}$. Then $(E_{3N}, \gamma_{3N})$ descends to $\mathcal{S}$ by finite étale descent since it is “invariant” under the action of $K$. The resulting elliptic curve with level-$N$ structure on $\mathcal{S}$ will serve as the universal object, and we denote it by $(E_N, \gamma_N)$. Now suppose we have a locally noetherian $\mathbb{Z}[1/3N]$-scheme $S$, and an elliptic curve with level-$N$-structure $(E, \gamma)$ over $S$. Since $(3, N) = 1$, we have $E[3N] \cong E[3] \times E[N]$, and similarly $\mathbb{Z}/3NZ \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Therefore, for any $S$-scheme $T$, to give a level-$3N$ structure on $E_T$ compatibly with the prescribed level-$N$ structure $\gamma$ is the same as to give simply a level-$3$-structure on $E_T$. Thus we have a map $\varphi : I_{E/S,3} \to S(3N)$, where for any level-$3$-structure we “combine” it with $\gamma$ to produce a level $3N$-structure. Now $\varphi$ is $K$-equivariant (with $K \cong \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ acting non-trivially on both sides), and therefore it descends to a map $\psi : S \to \mathcal{S}$ (by finite étale descent, using that $I_{E/S,3}$ is an étale $K$-torsor on $S$). One then checks that $\psi$ is the unique map that pulls $(E_N, \gamma_N)$ back to $(E, \gamma)$ up to isomorphism.

Similarly, we construct $S(N)_{\mathbb{Z}[1/2N]}$ as the quotient of $S(4N)$ (which is already constructed in Case (b)) by $\ker(\text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z}))$. Then we glue the two constructions to obtain $S(N)$ over $\mathbb{Z}[1/N]$ as we have already explained. By construction and finite étale descent, $S(N)$ is affine, smooth, of pure relative dimension 1 over $\mathbb{Z}[1/N]$.

Case (d): We are left with the case where $N = 2d$, with $d$ coprime to 6. By Case (c) we already have $S(d)$ over $\mathbb{Z}[1/d]$. Since $d|N$, we can construct $S(N)$ from $S(d)$ in the same way as how we constructed $S(N)$ from $S(3)$ in Case (a). (Note that since $(2, d) = 1$, we in fact have $S(N) \cong I_{E_{d}/S(d),1/2}$ by the decomposition $E[N] = E[d] \times E[2]$ for any elliptic curve $E$ over any locally noetherian $\mathbb{Z}[1/N]$-scheme $S$.)

---

6More precisely, for any $k \in K$, writing $f_k$ for the automorphism of $S(3N)$ given by $k$, we have a canonical isomorphism $f_k^*(E_{3N}, \gamma_N' \circ \cdot k^{-1}) = (E_{3N}, \gamma_N' \circ k^{-1})$. These isomorphisms satisfy the cocycle relation and therefore give rise to a descent datum.
Statement (1) in the following lemma is used for several times in the above proof of Theorem 17.2.1.

Lemma 18.1.1. Let \( N \geq 3 \). Let \( E \) be an elliptic curve over \( S \), and \( \gamma \) be a level-\( N \) structure on \( E \). The following statements hold.

(1) Let \( N' \) be a positive multiple of \( N \). For any level \( N' \)-structure \( \gamma' \) on \( E \), denote by \( \gamma'|_N \) the level-\( N \) structure induced by \( \gamma' \) (as explained in Case (a) in the proof of Theorem 17.2.1). Then the natural map

\[
\{ \gamma' \mid \gamma' \text{ is a level-}N' \text{ str. on } E, \gamma'|_N = \gamma \}
\rightarrow \{(E', \gamma') \text{ ell. cv. with level } N'-\text{str. on } S \mid (E', \gamma'|_N) \cong (E, \gamma)\}/\text{isom}
\]

is a bijection. Here on the right hand side we quotient out by the isomorphisms between elliptic curves with level-\( N' \) structures.

(2) The pair \((E, \gamma)\) has no non-trivial automorphism, i.e., the only automorphism of \( E \) (as an elliptic curve over \( S \)) preserving \( \gamma \) is the identity.

Proof. We first show that (2) implies (1). Clearly the two sets in (1) are simultaneously empty or non-empty, and when they are non-empty the map in question is surjective. To show injectivity, suppose \( \gamma' \) and \( \gamma'' \) are two elements of the left hand side such that \((E, \gamma') \cong (E, \gamma'')\). Thus there is an automorphism \( \tau \) of \( E \) carrying \( \gamma' \) to \( \gamma'' \). Since \( \gamma'|_N = \gamma''|_N = \gamma \), we see that \( \tau \) preserves \( \gamma \), and therefore must be the identity by (2). It follows that \( \gamma' = \gamma'' \).

We now prove (2). By the rigidity of the endomorphisms of \( E \) (see Fact 16.1.2), it suffices to treat the case where \( S \) is the spectrum of an algebraically closed field \( k \). In this case the statement is classical, but we give a proof.

Let \( H = \text{End}(E) \). This is a \( \mathbb{Z} \)-algebra, and is a free \( \mathbb{Z} \)-module of rank 2 or 4. Moreover, the \( \mathbb{Q} \)-algebra \( H \otimes_{\mathbb{Z}} \mathbb{Q} \) is either a quadratic imaginary field or a quaternion algebra over \( \mathbb{Q} \) ramified at \( \infty \) and \( p \), with the latter happening only when \( \text{char } k = p \). Now for any \( h \in H \), either \( h \in \mathbb{Z} \) or the minimal polynomial \( P_h(T) \) of \( h \) over \( \mathbb{Q} \) is a degree 2 monic polynomial in \( \mathbb{Z}[T] \). (Here \( h \) is integral over \( \mathbb{Z} \) since \( H \) is a finite \( \mathbb{Z} \)-module.)

We have \( \text{Aut}(E) = H^\times \), and by the previous description of \( H \) we know that \( \text{Aut}(E) \) is finite. Let \( g \in \text{Aut}(E) \) and suppose that \( g \) preserves \( \gamma \). Then \( g \) acts trivially on \( E[N] \). If \( g \in \mathbb{Z} \), then \( g = \pm 1 \), and then \( g = 1 \) since \(-1 \) does not act trivially on \( E[N] \) (as \( N \geq 3 \)). We may thus assume that \( g \notin \mathbb{Z} \). Then \( P_h(T) \) is a quadratic monic irreducible polynomial in \( \mathbb{Z}[T] \) whose roots are roots of unity (since \( g \) is of finite order), and therefore it must be one of the following:

\[
T^2 + 1, T^2 - T + 1, T^2 + T + 1.
\]

On the other hand the fact that \( g \) acts trivially on \( E[N] \) implies that \( g - 1 \in N \cdot H \), i.e., \( \frac{g-1}{N} \in H \). It is easy to see that

\[
P_g(T) = N^2 P_{\frac{g-1}{N}}(\frac{T-1}{N}).
\]

Since \( P_{\frac{g-1}{N}}(T) \) is monic integral, we see that

\[
P_g(T) \equiv T^2 - 2T + 1 \mod N.
\]

But this is not true for the three candidates of \( P_g(T) \), contradiction. \( \square \)

19. Lecture 19

We reviewed some key points from last lecture, including Case (c) in the proof of Theorem 17.2.1, and Lemma 18.1.1 (1).
19.1. Abelian schemes. We would like to generalize the modular curves to the higher-dimensional **Siegel modular varieties**. These are moduli spaces of polarized abelian schemes with level structure. Our next goal is to prove that such a moduli functor is indeed representable over a base like \( \mathbb{Z}[1/N] \), generalizing Theorem 17.2.1.

From now on, all schemes are assumed to be locally noetherian.

**Definition 19.1.1.** Let \( S \) be a scheme. An **abelian scheme** over \( S \) is a smooth proper group scheme over \( S \) all of whose geometric fibers are connected.

One can prove several useful facts about abelian schemes using the following Rigidity Lemma, which is a (more powerful) variant of Theorem 16.1.3.

**Theorem 19.1.2** (Rigidity Lemma). Let \( S \) be a scheme, and \( G \) be a group scheme over \( S \) and separated over \( S \). Let \( f : X \to S \) be a scheme morphism such that

1. \( f \) is flat.
2. either \( f \) is proper, or \( f \) is closed and admits a section.
3. For each \( s \in S \), the \( k(s) \)-vector space \( H^0(X_s, \mathcal{O}_{X_s}) \) is 1-dimensional.

Then for any two \( S \)-morphisms \( \phi, \phi' : X \to G \), if \( \phi \) and \( \phi' \) agree on one geometric fiber (or equivalently, on one fiber) for each connected component of \( S \), then \( \phi \) and \( \phi' \) differ by multiplication by a section in \( G(S) \).

**Proof.** See [MFK94, Prop. 6.1]. (Note that in loc. cit. all schemes are assumed to be separated over Spec \( \mathbb{Z} \), so all scheme maps are automatically separated.) \( \square \)

**Remark.** In Theorem 19.1.2, if \( f \) is flat and proper, then assumption (3) implies that the natural map \( \mathcal{O}_S \to f_*\mathcal{O}_X \) is an isomorphism. Thus in this case the set of assumptions on \( f \) is strictly stronger than Theorem 16.1.3 (where \( f \) is not assumed to be flat whatsoever). Also, in Theorem 16.1.3 the group scheme \( G \) is not assumed to be separated over \( S \). In any case, the assumptions on \( f \) in Theorem 19.1.2 are satisfied if \( f \) is flat proper with connected and reduced geometric fibers.

We have the following interesting consequence, which tells us that we can “separate variables” for \( G \)-valued functions in two variables under suitable assumptions.

**Corollary 19.1.3.** Let \( X \) and \( G \) over \( S \) be as in Theorem 19.1.2. Assume either that \( X \to S \) is proper, or that it is universally closed and admits a section. Let \( Y \) be a connected scheme over \( S \) and assume that \( Y \to S \) admits a section \( \epsilon \). Then for any \( S \)-scheme morphism \( \varphi : X \times_S Y \to G \), there are \( S \)-scheme morphisms \( g : X \to G \) and \( h : Y \to G \) such that \( \varphi \) is given by \( (x, y) \mapsto g(x) \cdot h(y) \).

20. Lecture 20

20.1. Abelian schemes, continued. We continue to assume all schemes are locally noetherian.

**Proof of Corollary 19.1.3.** Let \( f : X \to S \) be the structure map. We consider the following commutative diagram

\[
\begin{array}{ccc}
X \times_S Y & \xrightarrow{\phi} & G \times_S Y \\
\downarrow{\phi'} & & \downarrow{h} \\
Y & \xrightarrow{\epsilon} & G
\end{array}
\]
where we define
\[ \Phi(x, y) := (\varphi(x, y), y), \quad \Phi'(x, y) = (\varphi(x, \epsilon(f(x))), y). \]
The \( Y \)-scheme \( X \times_Y Y \) and the \( G \)-group scheme \( G \times_Y Y \) satisfy the hypotheses of Theorem 19.1.2. Now \( \Phi, \Phi' \) are \( Y \)-morphisms and for any \( y_0 \in \text{im}(\epsilon) \), the morphisms \( \Phi \) and \( \Phi' \) agree on the fiber of \( X \times_Y Y \) over \( y_0 \). Hence by Theorem 19.1.2 we know that \( \Phi, \Phi' \) differ by multiplication by a section of \( G \times_Y Y \) to \( Y \), which is of the form \( y \mapsto (h(y), y) \) for some \( S \)-map \( h : Y \to G \). Then we have \( \varphi(x, y) = \varphi(x, \epsilon(f(x))) \cdot h(y) \). Setting \( g(x) := \varphi(x, \epsilon(f(x))) \) we can conclude the proof.

Recall that an abelian scheme is a proper smooth group scheme with connected geometric fibers.

**Corollary 20.1.1.** Suppose \( X/S \) is an abelian scheme and \( G/S \) is a separated group scheme. Any \( S \)-map \( \varphi : X \to G \) preserving the neutral section is a group homomorphism. In particular, the group structure on \( X \) is determined by the neutral section.

**Proof.** We may assume that \( S \) is connected. Then \( X \) is connected, since \( X \to S \) is closed, surjective, and has connected fibers. Consider the composition
\[ \Phi : X \times_S X \xymatrix{ightarrow^\Phi \ar@{^{(}->}[r]_\mu & G \}
\]
where \( \mu \) is the multiplication map, i.e., \( \Phi(x, y) = \varphi(x \cdot y) \). Then by Corollary 19.1.3, we have \( \varphi(x \cdot y) = g(x) \cdot h(y) \) for some \( g : X \to G \) and \( h : X \to G \). Now observe that\[ e = \varphi(e \cdot e) = g(e)h(e). \]
This implies that \( h(e) = g(e)^{-1} \). Then we have \( \varphi(x) = \varphi(x \cdot e) = g(x)h(e) = g(x)g(e)^{-1}. \)
Also, \( \varphi(x) = \varphi(e \cdot x) = g(e)h(x). \)
So we have \( g(x) = \varphi(x)g(e), \quad h(x) = g(e)^{-1}\varphi(x). \)
Hence we have \( \varphi(x \cdot y) = g(x)h(y) = \varphi(x)g(e)g(e)^{-1}\varphi(y) = \varphi(x)\varphi(y). \)
This concludes. \( \square \)

**Corollary 20.1.2.** Suppose \( X/S \) is an abelian scheme. Then the group structure is commutative.

**Proof.** Apply Corollary 20.1.1 to the inversion \( X \to X, x \mapsto x^{-1}. \) \( \square \)

20.2. **Picard schemes.** Again we demand all schemes to be locally noetherian.

For a scheme \( X \), we define \( \text{Pic}(X) \) to be the abelian group of isomorphism classes of invertible \( O_X \)-modules. A morphism \( f : X \to Y \) of schemes gives a group homomorphism \( \text{Pic}(Y) \to \text{Pic}(X) \) via \( L \mapsto f^*L \). This yields the **absolute Picard functor** \( \text{Pic} : (\text{Sch})^{\text{op}} \to (\text{Ab}). \)

Suppose \( f : X \to S \) is a scheme morphism. It will be easier to work with the **relative Picard functor**, defined as\[ \text{Pic}_{X/S} : (S\text{-schemes})^{\text{op}} \to (\text{Ab}), \quad T \mapsto \text{Pic}(X_T)/f_T^*\text{Pic}(T), \]
where \( X_T := X \times_S T \) and \( f_T : X_T \to T \) is the base change of \( f \).
Theorem 20.2.1 (Grothendieck). Suppose $X \to S$ is a flat projective morphism with all geometric fibers integral (irreducible and reduced). Also assume that $X/S$ has a section. Then $\text{Pic}_{X/S}$ is representable by a commutative group scheme over $S$ which is locally of finite type and separated over $S$.

Proof. See [Kle05, Thm. (9.)4.8]. □

Remark. (1) If $e \in X(S)$ is a section, then $\text{Pic}_{X/S} \cong \text{Pic}_{X/S,e}$ where $\text{Pic}_{X/S,e}$ is the rigidified Picard functor sending each $S$-scheme $T$ to the group of isomorphism classes of pairs $(\mathcal{L}, \rho)$, where $\mathcal{L}$ is a line bundle on $X_T$ and $\rho$ is an isomorphism $e_T^* \mathcal{L} \sim \mathcal{O}_T$ (called a rigidification of $\mathcal{L}$ along $e_T$). Here, $e_T$ denotes the section of $X_T \to T$ induced by the section $e$ of $X \to S$. More explicitly, we have inverse bijections

$$\text{Pic}(X_T)/f_T^* \text{Pic}(T) \leftrightarrow \text{Pic}_{X/S,e}(T)$$

$$\mathcal{L} \leftrightarrow (\mathcal{L}, \rho)$$

$$\mathcal{L} \mapsto (\mathcal{L} \otimes f_T^* e_T^* \mathcal{L}^{-1}, \text{canonical } \rho).$$

Here the canonical $\rho$ is defined by noting that $e_T^*(\mathcal{L} \otimes f_T^* e_T^* \mathcal{L}^{-1})$ is canonically isomorphic to $e_T^* \mathcal{L} \otimes e_T^* \mathcal{L}^{-1}$.

(2) Without assuming the existence of a section but with the other assumptions in force, the theorem still holds for the fppf-sheafification (or just the étale sheafification) of $\text{Pic}_{X/S}$. See the discussion in [Kle05, §§3–4].

21. Lecture 21

21.1. Projective morphisms. Recall that a morphism $f : X \to S$ is called projective, if the $S$-scheme $X$ is isomorphic to a closed subscheme of the projective bundle $\mathbb{P}(E)$ over $S$ attached to some coherent $\mathcal{O}_S$-module $E$ on $S$. We caution the reader that in general this is not the same as requiring that $X$ is isomorphic to a closed subscheme of $\mathbb{P}_S^n$ for some $n$. However, when $S$ admits an ample invertible sheaf (e.g., when $S$ is affine), the two definitions are the same; see for instance [Sta18, Tag 0B45].

If $f : X \to S$ is projective, then it is proper, and there is an open covering $(U_i)$ of $S$ such that $X|_{U_i}$ is $U_i$-isomorphic to a closed subscheme of $\mathbb{P}_{U_i}^n$ for each $i$ (see [Sta18, Tag 01WE]). The converse is not true. Thus a locally projective morphism (i.e., one that becomes projective after passing to an open covering of the target) need not be projective.

21.2. The torsion component of the Picard scheme. The following result enhances Theorem 20.2.1.

Theorem 21.2.1 (Grothendieck). Let $f : X \to S$ be a flat projective morphism whose geometric fibers are integral. Assume $f$ admits a section, and that $f$ is smooth. Assume that $S$ is noetherian. Then there is a closed and open subgroup scheme $\text{Pic}_{X/S}^\tau$ of $\text{Pic}_{X/S}$ (over $S$), called the torsion component, satisfying the following conditions:

1. For each $s \in S$, the fiber of $\text{Pic}_{X/S}^\tau$ over $s$ consists of the torsion connected components of $(\text{Pic}_{X/S})_s$. Here we say that a connected component is torsion if its image under the multiplication-by-$n$ map $[n] : (\text{Pic}_{X/S})_s \to (\text{Pic}_{X/S})_s$ lies in the identity connected component for some $n \geq 1$.

2. $\text{Pic}_{X/S}^\tau$ is projective over $S$.

Proof. See [Kle05, Thm. 9.6.16, Exc. 9.6.18]. (It seems that the necessity of the assumption that $S$ is noetherian is overlooked in Grothendieck’s original article [Gro62, Cor. 4.2].) □
21.3. Dual abelian schemes. Now if $X/S$ is an abelian scheme, then all the assumptions in Theorem 20.2.1 are satisfied. If we assume that $X/S$ is projective and that $S$ is noetherian, then the assumptions in Theorem 21.2.1 are satisfied as well. Furthermore we have the following result:

**Theorem 21.3.1.** Let $X/S$ be a projective abelian scheme, and assume that $S$ is noetherian. Then $\text{Pic}^\tau_{X/S}$ is smooth and has connected geometric fibers. Hence in view of Theorem 21.2.1 we know that $\text{Pic}^\tau_{X/S}$ is a projective abelian scheme.

**Proof.** To show that $\text{Pic}^\tau_{X/S}$ has connected geometric fibers, we reduce to the case where $S$ is the spectrum of an algebraically closed field (since the formation of $\text{Pic}^\tau_{X/S}$ commutes with base change). Then this is a fundamental result in the theory of abelian varieties over a field; see [Mum08, §13]. The proof that $\text{Pic}^\tau_{X/S}$ is smooth is found in [MFK94, Prop. 6.7]. □

**Definition 21.3.2.** In the setting of Theorem 21.3.1, we call $\text{Pic}^\tau_{X/S}$ the dual abelian scheme of $X$, and denote it by $X^\vee$.

**Remark.** For an abelian variety $X$ over a field $k$, it is a classical result that $\text{Pic}^\tau_{X/k}$ is (geometrically) connected. Hence for an abelian scheme $X/S$ one could equivalently define $X^\vee$ by requiring that fiberwise it is the identity connected component of $(\text{Pic}_{X/S})_s$. (Note that the identity connected component of $(\text{Pic}_{X/S})_s$ is automatically geometrically connected since it has a rational point.) One can interpret the definition of $X^\vee$ as a subfunctor of $\text{Pic}_{X/S}$, even without knowing that $\text{Pic}_{X/S}$ is representable. Namely, for each $S$-scheme $T$ we declare that an element $\xi \in \text{Pic}_{X/S}(T)$ belongs to $X^\vee(T)$ if for every geometric point $\text{Spec} \ k \to T$ there exist a connected $k$-scheme $V$ and an element of $\text{Pic}_{X/S}(V)$ which specializes to $\xi$ and to 0 at two $k$-points of $V$. Hence for an arbitrary abelian scheme $X/S$ one could ask whether the functor $X^\vee$ is represented by an abelian scheme, even without requiring that $\text{Pic}_{X/S}$ is representable.

To answer this question, first we have a relatively easy generalization of Theorem 21.3.1: For any locally projective abelian scheme $X$ over any (locally noetherian) $S$, $\text{Pic}^\tau_{X/S}$ is a locally projective abelian scheme. This would immediately follow from Theorem 21.3.1 once we check that $X^\vee$ is a Zariski sheaf. A much deeper generalization is to drop all the assumptions whatsoever: For any abelian scheme $X$ over any $S$, $X^\vee$ is an abelian scheme. (This holds even without assuming that $S$ is locally noetherian.) This result is due to Raynaud and Deligne on top of Artin’s general result on the representability of Pic by algebraic spaces; see [FC90, §I.1].

21.4. Isogenies.

**Definition 21.4.1.** Let $A, B$ be two abelian schemes over an arbitrary (locally noetherian) $S$. By an isogeny, we mean an $S$-group scheme homomorphism $A \to B$ that is surjective and quasi-finite.

**Lemma 21.4.2.** Any isogeny $\phi : A \to B$ is finite and flat.

**Proof.** Since both $A$ and $B$ are proper over $S$, we know that $\phi$ is proper. But a proper and quasi-finite map is finite ([Sta18, Tag 02LS]), so $\phi$ is finite.

Since both $A$ and $B$ are flat and finite-type over $S$, we have the fiberwise criterion for flatness. Namely, in order to check that $\phi : A \to B$ is flat, we only need to check that $\phi_s : A_s \to B_s$ is flat for each $s \in S$. (See [Gro66, (11.3.11)] or [Sta18, Tag 039E].) Hence we reduce to the case where $S$ is the spectrum of a field $k$. We may also assume that $k$ is algebraically closed since flatness satisfies fpqc descent (see [Gro65, (2.2.11) (iv)] or [Sta18,
Tag 02L2). Now $\phi$ is a surjective map between two finite-type schemes over a field, and the target is integral. Hence we have the generic flatness (see [Gro65, §6.9]): There exists a non-empty open subscheme $U \subset B$ over which $\phi$ is flat. Since $\phi$ is a group homomorphism, we can use the group structure on $B$ to translate $U$, in order to obtain an open covering of $B$ such that $\phi$ is flat over each member of the covering. (For this step we need to use that $k$ is algebraically closed.) It follows that $\phi$ is flat, as desired. □

22. Lecture 22

22.1. The Mumford A-construction. Let $S$ be a noetherian scheme, and $f : A \to S$ a projective abelian scheme over $S$. For any line bundle $L$ on $A$, we define the Mumford line bundle $\mathfrak{M}(L)$ on $A \times_S A$ by

$$\mathfrak{M}(L) := \mu^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1},$$

where $p_1, p_2$ are the two projections $A \times_S A \to A$, and $\mu$ is the group law $A \times_S A \to A$.

Recall that for any $S$-scheme $T$ to give an $S$-map $T \to \text{Pic}_{A/S}$ is the same as to specify an element of $\text{Pic}(A_T)^* = \text{Pic}(T)$, where $A_T = A \times_S T$. Thus for $T = A$, the Mumford line bundle $\mathfrak{M}(L)$ on $A \times_S A = A_A$ gives rise to an $S$-map

$$\Lambda(L) : A \to \text{Pic}_{A/S}.$$

Lemma 22.1.1. The $S$-map $\Lambda(L)$ takes the neutral section of $A$ to the neutral section of $\text{Pic}_{A/S}$.

Proof. Let $e \in A(S)$ be the neutral section. To compute $\Lambda(L) \circ e$, we need to compute the pullback of $\mathfrak{M}(L)$ under

$$A = A \times_S S \xrightarrow{(\text{id}, e)} A \times_S A, \quad x \mapsto (x, e(f(x))).$$

Note that the compositions of the above map followed by $\mu, p_1, p_2 : A \times_S A \to A$ respectively are $\text{id}, \text{id}, e \circ f$. Hence the pullback of $\mathfrak{M}(L)$ under the above map is isomorphic to $f^*e^*L^{-1}$.

This line bundle on $A$ represents the zero element of $\text{Pic}_{A/S}(S) = \text{Pic}(A)/f^*\text{Pic}(S)$. Hence $\Lambda(L) \circ e$ is the neutral section of $\text{Pic}_{A/S}$. □

As a consequence, we know that $\Lambda(L) : A \to \text{Pic}_{A/S}$ is a group homomorphism by the Rigidity Lemma (see Corollary 20.1.1). Moreover, by the fiberwise connectedness of $A$, we know that $\Lambda(L)$ is a homomorphism $A \to A'$. Similarly to the proof of the above lemma, one shows that for two line bundles $L, M$ on $A$ we have

$$\Lambda(L \otimes M^{\pm 1}) = \Lambda(L) \pm \Lambda(M).$$

22.2. The case over an algebraically closed field. We now assume that $A$ is an abelian variety over an algebraically closed field $k$. In this case $A$ is automatically projective. (Strictly speaking for our course we do not need this information, because we will be exclusively working with abelian schemes $A/S$ which are assumed to be projective; in any case in the following we assume that $A/k$ is projective.)

Note that $\text{Pic}_{A/k}(k) = \text{Pic}(A)$, since $\text{Pic}(k)$ is trivial.

Let $L$ be a line bundle on $A$. It is easy to see that at the level of $k$-points the map $\Lambda(L)$ is given by

$$A(k) \to A' \subset \text{Pic}_{A/k}(k) = \text{Pic}(A), \quad x \mapsto t_x^*L \otimes L^{-1},$$

where $t_x : A \to A$ is translation by $x$. The fact that $\Lambda(L)$ is a group homomorphism thus entails the following:
Theorem 22.2.1 (Theorem of Square). For any line bundle \( L \) on \( A \) and any \( x, y \in A(k) \), we have an isomorphism of line bundles
\[
t^x_*L \otimes L \cong t^y_*L \otimes t^y_*L.
\]

We make two further observations.

Lemma 22.2.2. Let \( L \) be a line bundle on \( A \). Then \( \Lambda(L) = 0 \) if and only if the Mumford line bundle \( \mathcal{M}(L) \) is trivial.

Proof. The “if” direction is clear from the very definition of \( \Lambda(L) \) in terms of \( \mathcal{M}(L) \). Suppose that \( \Lambda(L) = 0 \). Then we know, again by the definition of \( \Lambda(L) \), that \( \mathcal{M}(L) \) dies in \( \text{Pic}(A \times_k A)/p_2^*\text{Pic}(A) \). In general, suppose \( M \) is a line bundle on \( A \times_k T \) which isomorphic to \( p_2^*(N) \) for some line bundle \( N \) on \( T \). Write \( e_T \) for the map \( T \to A \times_k T, t \mapsto (c, t) \). Then
\[
p_2^*e_T M \cong p_2^*e_T p_2^*N \cong p_2^*N \cong M,
\]
where the second isomorphism is because \( p_2 \circ e_T = \text{id}_T \). In particular,
\[
M \otimes p_2^*e_T M^{-1} \cong \mathcal{O}_{A \times T}.
\]
Applying this to \( M = \mathcal{M}(L) \), we know that
\[
\mathcal{M}(L) \otimes p_2^*(e_2, \text{id})^*\mathcal{M}(L)^{-1} \cong \mathcal{O}_{A \times A}.
\]
A computation shows that the left hand side is isomorphic to \( \mathcal{M}(L) \otimes e_2^*L \), where \( e_2 \) is the map \( A \times_k A \to A, (x, y) \mapsto e \). But \( e_2^*L \) is trivial since \( e_2 \) factors through \( \text{Spec} k \) and \( \text{Pic}(k) = 0 \). Hence \( \mathcal{M}(L) \) is trivial.

Since \( A/k \) is projective, it has ample line bundles.

Lemma 22.2.3. Let \( L \) be an ample line bundle on \( A \). Then \( \ker(\Lambda(L)) \) is a finite subgroup scheme of \( A \).

Proof. Suppose not. Then one can find a positive-dimensional abelian subvariety \( B \subset A \) contained in \( \ker(\Lambda(L)) \). Note that \( \Lambda(L)|_B = \Lambda(L|_B) \), and \( L|_B \) is ample on \( B \). Thus for the sake of deducing a contradiction we may assume that \( B = A \), i.e., \( \Lambda(L) = 0 \). By Lemma 22.2.2, \( \mathcal{M}(L) \) is trivial. The pullback of \( \mathcal{M}(L)^{-1} \) along the “anti-diagonal”
\[
(id, [-1]): A \to A \times_k A, \quad x \mapsto (x, -x)
\]
is \( L \otimes [-1]^*L \), and it must be trivial on \( A \). Since \( L \) is ample and \([-1]\) is an automorphism of \( A \), \( L \otimes [-1]^*L \) is ample. Thus the trivial line bundle on \( A \) is ample, a contradiction with the fact that \( A \) is projective and positive-dimensional.

The following is the “main theorem” for line bundles on an abelian variety.

Theorem 22.2.4 (Main Theorem). Fix an ample line bundle \( L \) on \( A \). For any line bundle \( M \) on \( A \), we have \( \Lambda(M) = 0 \) if and only if \( M \cong \Lambda(L) |_x = t^x_*L \otimes L^{-1} \) for some \( x \in A(k) \).

The proof of the above theorem will be given in the future few lectures. Let us now deduce some important consequences.

Definition 22.2.5. Let \( M, M' \) be two line bundles on \( A \). We say that \( M \) is algebraically equivalent to \( M' \), if there exists a connected \( k \)-scheme \( T \) and a line bundle on \( A \times_k T \) specializing to \( M \) and \( M' \) at two \( k \)-points of \( T \).

Lemma 22.2.6. Two line bundles \( M \) and \( M' \) are algebraically equivalent if and only if the isomorphism class of \( M \otimes M'^{-1} \) lies in \( \text{Pic}(A) \subset \text{Pic}_{A/k}(k) = \text{Pic}(A) \).
Proof. Exercise. (Use the moduli interpretation of Pic_{A/k}.)

The following corollary of Theorem 22.2.4 says that one can detect algebraic equivalence of line bundles by looking at Λ(λ).

**Corollary 22.2.7.** Let M be a line bundle on A. Then M is algebraically equivalent to zero if and only if Λ(M) = 0.

We will prove this next time.

23. Lecture 23

23.1. **Criterion for algebraic equivalence.** Let A be an abelian variety over an algebraically closed field k. The following two corollaries are consequences of Theorem 22.2.4.

**Corollary 23.1.1.** Let M be a line bundle on A. Then M is algebraically equivalent to zero if and only if Λ(M) = 0.

**Proof.** Suppose M is algebraically equivalent to zero. Then there is a connected k-scheme T and a line bundle ˜M on A × T which specializes to M and to O_A at two points t_1, t_2 ∈ T(k). Consider the T-group scheme homomorphism

Λ(˜M) : A_T = A × T −→ Pic_{A_T/T}.

On the fiber of A_T over t_2, the map induced by Λ(˜M) is Λ(O_A) = 0. Thus Λ(˜M) and the zero homomorphism agree on one fiber over T. Since they both preserve the neutral section, they must be equal by the Rigidity Lemma (see Theorem 19.1.2). Thus Λ(˜M) = 0. But on the fiber over t_1, the map induced by Λ(˜M) is Λ(M). Hence Λ(M) = 0.

Conversely, suppose that Λ(M) = 0. Then by Theorem 22.2.4, there exists an (ample) line bundle L on A and a point x ∈ A(k) such that M = Λ(L)(x). But Λ(L)(A(k)) ⊂ A^∨(k), so M ∈ A^∨(k). Thus M is algebraically equivalent to zero by Lemma 22.2.6.

**Corollary 23.1.2.** Let L be an ample line bundle on A. Then Λ(L) : A → A^∨ is an isogeny.

**Proof.** By Lemma 22.2.3, Λ(L) is quasi-finite. To see that it is surjective, let M ∈ A^∨(k). Then Λ(M) = 0 by Corollary 23.1.1. Hence M ∈ im(Λ(L)) by Theorem 22.2.4.

The above two corollaries will be the essential tools needed to study “polarizations”. Note that these they together imply the “only if” direction of Theorem 22.2.4, which is the more difficult direction.

23.2. **Proof of Theorem 22.2.4.** We first show the “if” direction. Suppose M = t^*_y L ⊗ L^{-1}. Then for any y ∈ A(k) we compute

Λ(M)(y) = t^*_y M ⊗ M^{-1} ∼= t^*_{x+g} L ⊗ t^*_y L^{-1} ⊗ t^*_y L^{-1} ⊗ L,

which is trivial by the Theorem of Square (Theorem 22.2.1). Thus Λ(M) = 0. This proves the “if” direction.

For the “only if” direction we need some preparations.

**Lemma 23.2.1.** Let M be a line bundle on A with Λ(M) = 0. Then for any k-scheme T and any two k-scheme maps f, g : T → A, we have (f + g)^* M ∼= f^* M ⊗ g^* M. (Here the addition in f + g is the group law.) For any n ∈ Z, we have [n]^* M ∼= M ⊗^n, where [n] is the multiplication-by-n map A → A, x ↦ x + ··· + x (n times).
Proof. By Lemma 22.2.2, \( \mathfrak{M}(M) \) is trivial. The pullback of \( \mathfrak{M}(M) \) along 
\[
(f, g) : T \longrightarrow A \times_k A
\]
is \( (f + g)^* M \otimes f^* M^{-1} \otimes g^* M^{-1} \), and this is trivial. This proves the first statement. For the second statement, note that it is obviously true for \( n = 0 \) or \( 1 \). (For \( n = 0 \), note that \( [0]^* \) of any line bundle is trivial since \( [0] : A \rightarrow A \) factors through \( \text{Spec} \ k \).) Applying the first statement to \( f = [m] \) (with \( m \geq 1 \)) and \( g = [1] \), we prove by induction that the statement holds for all \( n \geq 1 \). For negative \( n \), use that \( \mathcal{O}_A \cong [0]^* M \cong [n-n]^* M \cong [n]^* M \otimes [-n]^* M \). \( \square \)

Lemma 23.2.2. Let \( M \) be a line bundle on \( A \) with \( \Lambda(M) = 0 \). If \( M \) is non-trivial, then \( \mathbf{H}^j(A, M) = 0 \) for all \( j \geq 0 \).

Proof. We induct on \( j \). For \( j = 0 \), suppose \( \mathbf{H}^0(A, M) \neq 0 \). Then \( M \cong \mathcal{O}_A(-D) \) for some effective divisor \( D \). By Lemma 23.2.1, \( \mathcal{O}_A(D) \cong M^{-1} \cong [-1]^* M \cong \mathcal{O}_A([-1]^*(-D)) \), i.e., 
\[
\mathcal{O}_A \cong \mathcal{O}_A(D + [-1]^*) \approx D.
\]
But both \( D \) and \( [-1]^* D \) are effective, so \( D = 0 \), a contradiction with the non-triviality of \( M \).

For the induction step, assume \( j \geq 1 \). We factorize \( \text{id}_A \) as 
\[
A \overset{(\text{id}, \epsilon)}{\longrightarrow} A \times_k A \overset{\mu}{\longrightarrow} A.
\]
Thus the identity map on \( \mathbf{H}^j(A, M) \) factors through \( \mathbf{H}^j(A \times_k A, \mu^* M) \), and it suffices to prove that \( \mathbf{H}^j(A \times_k A, \mu^* M) = 0 \). Since \( \mathfrak{M}(M) \) is trivial (by Lemma 22.2.2), we have 
\[
\mathbf{H}^j(A \times_k A, \mu^* M) \cong \mathbf{H}^j(A \times_k A, p_1^* M \otimes p_2^* M).
\]
By the Künneth formula the above is isomorphic to 
\[
\bigoplus_{u+v=j} \mathbf{H}^u(A, M) \otimes_k \mathbf{H}^v(A, M),
\]
and this is zero by the induction hypothesis since for every pair \( (u, v) \) with \( u + v = j \) at least one of \( u, v \) is strictly less than \( j \). \( \square \)

We are now ready to prove the “only if” direction of Theorem 22.2.4. (The reference for this proof is [Mum08, §8, Thm. 1].) For the sake of contradiction suppose that \( \forall x \in A(k) \), \( M \) is not isomorphic to \( t_x^* L \otimes L^{-1} \). Define a line bundle on \( A \times_k A \):
\[
K := \mathfrak{M}(L) \otimes p_2^* M^{-1}.
\]
For any \( x \in A(k) \), we write \( K|_{\{x\} \times A} \) for the pullback of \( K \) along \( A \rightarrow A \times_k A, y \mapsto (x, y) \). We have 
\[
K|_{\{x\} \times A} \cong t_x^* L \otimes L^{-1} \otimes M^{-1},
\]
and this is non-trivial by our assumption. Now 
\[
\Lambda(K|_{\{x\} \times A}) = \Lambda(t_x^* L \otimes L^{-1} \otimes M^{-1}) = \Lambda(t_x^* L \otimes L^{-1}) - \Lambda(M).
\]
The first term is zero by the “if” direction of the theorem, and the second term is zero by assumption. Hence 
\[
\mathbf{H}^j(A, K|_{\{x\} \times A}) = 0, \quad \forall j \geq 0
\]
by Lemma 23.2.2. Since \( x \in A(k) \) is arbitrary, this implies that 
\[
R^j p_{1,*} K = 0, \quad \forall j \geq 0
\]
by “cohomology and base change”; see [Mum08, §5, Cor. 3]. (To use this result one needs to check that \( \mathbf{H}^j(\text{Spec} \ k(x) \times_{\text{Spec} \ k} A, K|_{\{x\} \times A}) = 0 \) for all points \( x \in A \), not just the closed
points. However by semi-continuity [Mum08, §5, Cor. 1] knowing the vanishing for all closed points \( x \in A(k) \) is already enough.) By the Leray spectral sequence

\[
E_2^{p,q} = H^p(A, R^q p_* K) \implies H^{p+q}(A \times_k A, K),
\]

we conclude that

\[
H^i(A \times_k A, K) = 0, \quad \forall i \geq 0.
\]

We now look at the other Leray spectral sequence

\[
E_2^{p,q} = H^p(A, R^q p_* K) \implies H^{p+q}(A \times_k A, K).
\]

For \( x \in A(k) \), we have

\[
K|_{A \times \{x\}} \cong t^*_x L \otimes L^{-1},
\]

and so \( \Lambda(K|_{A \times \{x\}}) = 0 \) again by the “if” direction of the theorem. If \( t^*_x L \otimes L^{-1} \) is non-trivial, i.e., \( x \notin \ker(\Lambda(L))(k) \), then again by Lemma 23.2.2 we have

\[
H^j(K|_{A \times \{x\}}) = 0, \quad \forall j \geq 0.
\]

Hence for each \( j \), \( R^j p_* K \) is supported on the closed subscheme \( \ker(\Lambda(L)) \subset A \). But \( L \) is ample, so \( \ker(\Lambda(L)) \) is a finite (maybe non-reduced) \( k \)-scheme by Lemma 22.2.3. Thus

\[
H^i(A, R^j p_* K) = 0, \quad \forall i \geq 1, \forall j \geq 0.
\]

Thus the only non-zero terms in the \( E_2 \)-page of the spectral sequence (23.1) are those in the 0-th row. It follows that

\[
H^0(A, R^j p_* K) = H^j(A \times_k A, K), \quad \forall j \geq 0.
\]

We have already seen that this is zero. Since \( R^j p_* K \) is finitely supported, we conclude that

\[
R^j p_* K = 0, \quad \forall j \geq 0.
\]

Again by “cohomology and base change” (see [Mum08, §5, Cor. 4]), this implies that for any \( x \in A(k) \), we have

\[
H^j(A, K|_{A \times \{x\}}) = 0, \quad \forall j \geq 0.
\]

Taking \( j = 0 \) and \( x = e \), we get \( H^0(A, \mathcal{O}_A) = 0 \), which is absurd since this should be \( k \). This finishes the proof of Theorem 22.4.

24. Lecture 24

24.1. Theorem of Cube and consequences.

**Theorem 24.1.1** (Theorem of Cube). Let \( X, Y, Z \) be three abelian varieties over a field \( k \) (not necessarily algebraically closed). Let \( L \) be a line bundle on \( X \times Y \times Z \) (all the products are over \( k \)) such that its restrictions to \( \{e\} \times Y \times Z \cong Y \times Z, X \times \{e\} \times Z \cong X \times Z, X \times Y \times \{e\} \cong X \times Y \) are all trivial. Then \( L \) is trivial.

**Proof.** Fix a trivialization \( \rho \) of \( L|_{X \times Y \times \{e\}} \). Then \( (L, \rho) \) defines an element of \( \text{Pic}_{Z/k,e}(X \times Y) \), or in other words a \( k \)-map \( F : X \times Y \to Z \). By Corollary 19.1.3, \( F \) is of the form \( F(x, y) = g(x) + h(y) \) for \( k \)-maps \( g : X \to Z \) and \( h : Y \to Z \). By our assumptions, we have

\[
g(e) + h(y) = g(x) + h(e) = 0 \quad \text{for all } x \in X, y \in Y.
\]

Thus \( g \) and \( h \) are constant (i.e., they factor through the structure maps \( X \to \text{Spec } k, Y \to \text{Spec } k \) respectively). Then \( F = 0 \), and so \( (L, \rho) \) represents the trivial element of \( \text{Pic}_{Z/k,e}(X \times Y) \), which in particular implies that \( L \) is trivial. \( \square \)
Corollary 24.1.2. Let $A$ be an abelian variety over a field $k$, and let $L$ be a line bundle on $A$. Let $T$ be a $k$-scheme, and $f, g, h : T \to A$ be $k$-maps. Then

$$(f + g + h)^* L \cong (f + g)^* L \otimes (g + h)^* L \otimes (f + h)^* L \otimes g^* L^{-1} \otimes h^* L^{-1}.$$  

Proof. Let $p_i$ be the $i$-th projection $A \times A \times A \to A$, and $p_{ij} := p_i + p_j : A \times A \times A \to A$. Let $m := p_1 + p_2 + p_3 : A \times A \times A \to A$. Define a line bundle on $A \times A \times A$:

$$M := m^* L \otimes p_{12}^* L^{-1} \otimes p_{13}^* L^{-1} \otimes p_{23}^* L^{-1} \otimes p_1^* L \otimes p_2^* L \otimes p_3^* L.$$  

Then the difference of the two sides of the desired isomorphism is the pullback of $M$ along

$$(f, g, h) : T \to A \times A \times A.$$  

Hence it suffices to check that $M$ is trivial. But one directly checks that $M$ satisfies the hypothesis in the Theorem of Cube. \qed

Corollary 24.1.3. Let $A$ and $L$ be as in Corollary 24.1.2. Then for each $n \in \mathbb{Z}$ we have

$$[n]^* L \cong L^{n^2} \otimes (L \otimes [-1]^* L^{-1})^{(n^2 - 1)/2}.$$  

Proof. Write $L_n$ for $[n]^* L$. Applying Corollary 24.1.2 to $f = [n + 1], g = [1], h = [-1]$, we get

$$L_{n+1} \cong L_{n+2} \otimes L_0 \otimes L_{n} \otimes L_{n+1}^{-1} \otimes L_1^{-1} \otimes L_1^{-1},$$  

i.e.,

$$L_{n+2} \otimes L_{n+1}^2 \otimes L_n \cong L \otimes L_{-1}.$$  

Note that the desired isomorphism obviously holds for $n = 0$ and $n = 1$. The proof is then done by induction in the two directions, i.e., knowing the desired formula for $L_n$ and $L_{n+1}$ we can compute $L_{n+2}$, and knowing the desired formula for $L_{n+2}$ and $L_{n+1}$ we can compute $L_n$. \qed

We say that a line bundle $L$ on $A$ is symmetric if $L \cong [-1]^* L$. If $L$ is symmetric, then $[n]^* L \cong L^{n^2}$. Now pick an ample line bundle $L_0$ and let $L = L_0 \otimes [-1]^* L_0$. Then $L$ is both ample and symmetric. In particular, on $A$ we have an ample line bundle $L$ such that $[n]^* L \cong L^{n^2}$. From this, it is easy to see that $[n] : A \to A$ is an isogeny. Moreover, for any ample line bundle $L$ on $A$ and any isogeny $f : A \to A$, we have $\deg(L) \neq 0$, $\deg(L^m) = m^\dim A \deg(L)$, $\forall m \geq 1$, and $\deg(f^* L) = \deg(f) \deg(L)$. It follows that $\deg([n]) = n^{2 \dim A}$. Here the degree of a line bundle is defined using the Hilbert polynomial; see [Mum08, Appendix to §6] for details.

The following result will be proved in the next lecture.

Corollary 24.1.4. Let $A$ be an abelian variety over an algebraically closed field $k$. For any ample line bundle $L$ on $A$, we have $\mathbb{H}^i(A, L) = 0$ for all $i > 0$.

25. Lecture 25

25.1. Cohomology of an ample line bundle. In the following, let $k$ be an algebraically closed field, and $A/k$ an abelian variety.

Corollary 25.1.1. For any line bundle $L$ on $A$ and any integer $n$, the line bundle $[n]^* L$ is algebraically equivalent to $L^{\otimes n}$.

Remark. Recall from Lemma 23.2.1 that if $L$ is a line bundle satisfying $\Lambda(L) = 0$, then $[n]^* L \cong L^{\otimes n}$. In this case $L$ is algebraically equivalent to zero, so this does not contradict with the current corollary.
Theorem 26.1.1. The following result.

Let $k$ be an algebraically closed field, and let $A$ be an abelian variety over $k$. Suppose $L$ is an ample line bundle on $A$. We want to show that $H^i(A, L^n) = 0$ for all $i > 0$.

Proof. By Corollary 24.1.3, we only need to show that $\Delta := L \otimes [-1]^* L^{-1}$ is algebraically equivalent to 0. By Corollary 23.1.1, we only need to show that $\Lambda(\Delta) = 0$. For any $x \in A(k)$, we compute

$$
\Lambda(\Delta)(x) \cong t_x^* L \otimes L^{-1} \otimes [-1]^* L^{-1} \otimes [-1]^* L \cong t_x^* L \otimes L^{-1} \otimes [-1]^* (t_x^* L^{-1} \otimes L)
$$

$$
\cong t_x^* L \otimes L^{-1} \otimes (t_x^* L^{-1} \otimes L)^{-1},
$$

where the last isomorphism is because $[-1]^* M \cong M^{-1}$ for all $M$ such that $\Lambda(M) = 0$ (see Lemma 23.2.1). The above is isomorphic to

$$
t_x^* L \otimes t_x^* L \otimes L^{-2},
$$

and this is isomorphic to $t_0^* L \otimes L^{-1} \cong O_A$ by the Theorem of Square. Hence $\Lambda(\Delta) = 0$. □

Corollary 25.1.2. For any ample line bundle $L$ on $A$, we have $H^i(A, L) = 0$ for all $i > 0$.

Proof. Since $L$ is ample, there is an integer $n_0$ such that

$$
H^i(A, L^n) = 0, \quad \forall i \geq 1, n \geq n_0.
$$

Suppose $L'$ is a line bundle algebraically equivalent to $L^n$. By Theorem 22.2.4, since $L' \otimes L^{-n}$ is algebraically equivalent to zero and since $L^n$ is ample, we know that $L' \otimes L^{-n} \cong t_x^* L^n \otimes L^{-n}$ for some $x \in A(k)$. Thus $L' \cong t_x^* L^n$, and so $H^i(A, L') = 0$ for all $i \geq 1$ since $t_x$ is an automorphism of $A$.

Now by Corollary 25.1.1, $[n]^* L$ is algebraically equivalent to $L^{n^2}$, so we have

$$
H^i(A, [n]^* L) = 0, \quad \forall i \geq 1, n \geq \sqrt{n_0}.
$$

But the above is also isomorphic to

$$
H^i(A, [n]^* L)
$$

since $[n] : A \to A$ is finite. We claim that if char $k$ does not divide $n$, then $L$ is a direct summand of $[n]^* L$. This would finish the proof since we can pick $n$ sufficiently large and not divisible by char $k$.

To prove the claim, first note that by the projection formula we have $[n]^* L \cong L \otimes [n]^* O_A$. Hence it suffices to show that $O_A$ is a direct summand of $[n]^* O_A$. Since $[n]$ is finite flat, there is a canonical trace map $[n]^* O_A \to O_A$ (see [Sta18, Tag 0BVH]) which when composed with the natural map $O_A \to [n]^* O_A$ on the left is the map $O_A \to O_A$ that multiplies each section by $\deg [n] \in \mathbb{Z}$. But $\deg [n] = n^{2 \dim A}$ is invertible over $A$, so the claim follows. □

26. Lecture 26

26.1. Global sections of ample line bundles. Let $A$ be an abelian variety over an algebraically closed field $k$ and take $L$ to be an ample line bundle on $A$. We showed last lecture that $H^i(A, L) = 0$ for all $i > 0$. We want now to show that for such $L$, we have the following result.

Theorem 26.1.1.

$$
\dim H^0(A, L) = \sqrt{\deg \Lambda(L)}.
$$

We first briefly examine the case of elliptic curves. If $A = E$ is an elliptic curve, we note that $L_1 = O(e)$ is a canonical choice of an ample line bundle, as $L_1 \otimes^3$ is very ample. In this case, we know that $\dim H^0(E, L_1) = 1$. Hence by the theorem we have $\deg \Lambda(L_1) = 1$, which in particular says that $\Lambda(L_1) : E \to E^\vee$ is an isomorphism. As such, we may canonically identify $E$ with $E^\vee$ via $\Lambda(L_1)$. 

Remark. We know that $\Lambda(L_1)$ is a group homomorphism, and on $k$-points it is given by $$E(k) \rightarrow E'(k), \quad P \mapsto t_\nu^*(\mathcal{O}(e)) \otimes \mathcal{O}(e)^{-1} = \mathcal{O}([P] - [e]).$$ Hence we once again see that the group structure on $E(k)$ is given by the following rule: We have $P + Q = R$ if and only if $\mathcal{O}([P] - [e]) \otimes \mathcal{O}([Q] - [e]) \cong \mathcal{O}([R] - [e])$, i.e., $[P] + [Q] - 2[e]$ is linearly equivalent to $[R] - [e]$.

On an elliptic curve $E$, consider more generally the line bundles $L_n := \mathcal{O}(n[e]) = L_{1/n}^\otimes$. Then $\Lambda(L_n) = n \cdot \Lambda(L_1) = [n] \circ \Lambda(L_1)$. If we use $\Lambda(L_1)$ to canonically identify $E$ and $E'$, then $\Lambda(L_n)$ is identified with $[n]$. Recall that by Riemann–Roch, we have $\dim H^0(E, L_n) = n$. We have also seen that $\deg[n] = n^2$. This verifies the theorem for $L_n$.

To prove Theorem 26.1.1 in general we need some preparations.

26.2. The Poincaré line bundle. Suppose $A/S$ is a projective abelian scheme where $S$ is noetherian. Recall that $\text{Pic}_{A/S}$ represents the rigidified Picard functor $$\text{Pic}_{A/S,e} : (\text{locally noetherian } S\text{-schemes}) \rightarrow (\text{Abelian groups})$$ given by $$T \mapsto \{(L, \rho) \mid L \text{ a line bundle on } A_T = A \times_S T, \rho : e_T^* L \sim \mathcal{O}_T\}/\cong.$$ Over $A_{\text{Pic}_{A/S}} = A \times_S \text{Pic}_{A/S}$, we have a universal pair $(L, \rho)$ where $L$ is a line bundle on $A_{\text{Pic}_{A/S}}$ and $\rho : (e, \text{id})^* L \sim \mathcal{O}_{A_{\text{Pic}_{A/S}}}$. This pair is unique up to isomorphism. We may restrict $(L, \rho)$ to $A \times_S A^\vee$. In particular, we acquire the so-called Poincaré line bundle $\mathcal{P}$ on $A \times_S A^\vee$, which comes equipped with a trivialization along $(e, \text{id})$.

Remark. Let $e^\vee$ be the neutral section of $A^\vee \rightarrow S$. Then $(\text{id}, e^\vee)^* \mathcal{P}$ on $A$ is also equipped with a trivialization and this trivialization is compatible with the previous trivialization in the sense that these two induce the same isomorphism $$(e, e^\vee)^* \mathcal{P} \sim \mathcal{O}_S.$$

Remark. We have the “flipping” identification $f : A^\vee \times A \sim A \times A^\vee, (x, y) \mapsto (y, x)$. Notice that $f^* \mathcal{P}$ is a line bundle on $A^\vee \times A$ again equipped with two compatible trivializations along $(e^\vee, \text{id})$ and $(\text{id}, e)$. We can use this structure to obtain a canonical map $A \rightarrow A^\vee$, which turns out to be an isomorphism.

Remark. The role played by the Poincaré line bundle in the duality theory for abelian varieties is analogous to the evaluation morphism $ev : V \otimes_k V^\vee \rightarrow k$ for a vector space $V$ over $k$.

Remark. Given an abelian variety $A/k$ where $k = \overline{k}$, we can pick (non-canonically) an ample line bundle $L$ to acquire an isogeny $\Lambda(L) : A \rightarrow A^\vee$. This in particular implies that $\dim A^\vee = \dim A$.

We will study the cohomology of $A \times A^\vee$ with coefficients in the sheaf $\mathcal{P}$ as an intermediate step in attacking Theorem 26.1.1.

Theorem 26.2.1. Suppose $A$ is an abelian variety over an algebraically closed field $k$ with dimension $g$. We have $$H^n(A \times_k A^\vee, \mathcal{P}) = \begin{cases} 0, & n \neq g \\ k, & n = g. \end{cases}$$
Proof. In the following we write $A \times A^\vee$ for $A \times_k A^\vee$. We consider $R^n p_{2, *} \mathcal{P}$ where $p_2 : A \times A^\vee \to A^\vee$ is the second projection. Note that for $x \in A^\vee(k) \setminus \{e^\vee\}$, the isomorphism class of the line bundle $\mathcal{P}|_{A \times \{x\}}$ on $A$ tautologically corresponds to $x \in \text{Pic}(A)$. Since we are assuming that $x$ is nontrivial, this line bundle must also be nontrivial and algebraically equivalent to 0. Hence, for such $x$, by Corollary 23.1.1 and Lemma 23.2.2, we have

$$H^n(A \times \{x\}, \mathcal{P}|_{A \times \{x\}}) = 0, \quad \forall n \geq 0.$$ 

In particular, for all $n \geq 0$, we know that $R^n p_{2, *} \mathcal{P}$ is supported at the neutral section $e^\vee$. By the Leray spectral sequence, we have

$$E_2^{p,q} = H^p(A^\vee, R^q p_{2, *} \mathcal{P}) \implies H^{p+q}(A \times_k A^\vee, \mathcal{P}).$$

Now $H^0(A^\vee, R^q p_{2, *} \mathcal{P}) = 0$ except when $p = 0$, since $R^q p_{2, *} \mathcal{P}$ is supported on a finite scheme. This yields

$$H^0(A^\vee, R^q p_{2, *} \mathcal{P}) \cong H^n(A \times A^\vee, \mathcal{P})$$

for all $n$. If $n > g$, then $R^n p_{2, *} \mathcal{P} = 0$ as $p_2$ has relative dimension $g$. Hence $H^n(A \times A^\vee, \mathcal{P}) = 0$ for $n > g$. Now notice that

$$\omega_{A \times A^\vee} = \wedge^{2g} \Omega_{A \times A^\vee/k}$$

is a trivial line; this is because $\Omega_{A \times A^\vee/k}$ is a trivial vector bundle already by the fact that $A \times A^\vee$ is an abelian variety (see [Mum08, §4 (iii)]). Hence by Serre duality applied to the $2g$-dimensional $A \times A^\vee$, we have

$$H^n(A \times A^\vee, \mathcal{P}) \cong H^{2g-n}(A \times A^\vee, \mathcal{P}^{-1})^\vee.$$ 

In particular, we know that $H^i(A \times A^\vee, \mathcal{P}^{-1})^\vee = 0$ for $i < g$. It is an easy exercise to show that

$$\mathcal{P}^{-1} \cong ([1], [−1])^* \mathcal{P}.$$ 

Since $([1], [−1]) : A \times A^\vee \to A \times A^\vee$ is an automorphism, this implies that $\mathcal{P}$ and $\mathcal{P}^{-1}$ have the same cohomology. Hence $H^n(A \times A^\vee, \mathcal{P}) = 0$ for all $n < g$ as well. It remains to show that $H^g(A \times A^\vee, \mathcal{P}) = k$. \hfill \Box

References


[FC90] Gerd Faltings and Ching-Li Chai. Degeneration of abelian varieties, volume 22 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1990. With an appendix by David Mumford. 43


