Abelian Varieties and Modular Forms on Symplectic Groups

Author:
Robert Sayer

Supervisor:
Dr. Alexandru Ghitza

Contents

1 Introduction: (Elliptic) Modularity

With the intent of getting ourselves properly oriented (and also of motivating the theory which is to come) we begin with a rapid introduction to the basic objects and phenomena of the Modularity Theorem of Taylor-Wiles and Taylor-Breuil-Conrad-Diamond.

1.1 Classical modular forms

Let $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ denote the upper half complex plane, and recall that $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$ by fractional linear transformations. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ ie. a subgroup containing the kernel of the (surjective) homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for some natural number N.

Definition 1.1. *Let k be a positive integer. A* **modular form** *of weight k and level Γ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying the following two conditions.*

(a) For all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $f(\gamma z) = (cz+d)^k f(z)$.

(b) f is "holomorphic at the cusps" *of Γ.*

A meromorphic function satisfying condition (a) is called a **weakly-modular** function of weight k and level Γ. Condition (b) requires some explanation. Since Γ is by assumption a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, it contains a matrix of the form

$$T^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$

which acts as $z \mapsto z + m$ on $\mathbb{H}$. Moreover, one has $f(T^m z) = f(z)$ for all $z \in \mathbb{H}$ and it follows that f possesses a Fourier expansion of the form

$$f(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n/m}.$$

One says that f is **holomorphic at infinity** if $a_n = 0$ for $n < 0$, ie. if the limit

$$\lim_{y \to \infty} f(iy)$$

exists. In general, a **cusp** of Γ is a Γ-orbit of points in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$[1]. Since $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$ for any congruence subgroup Γ the set of cusps is always finite. One says that f is **holomorphic at the cusps** of Γ if the function $f|_\gamma(z) = f(\gamma z)(cz+d)^{-k}$ (which is holomorphic and *a priori* weakly modular for $\gamma^{-1}\Gamma\gamma$) is holomorphic at infinity for each $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

The set of all modular forms of fixed weight k and level Γ is naturally a vector space over $\mathbb{C}$. We denote this space by $M_k(\Gamma)$ and remark that, by the Riemann-Roch theorem, such a space is always finite dimensional. Under pointwise addition and multiplication, the space $\bigoplus_{k \geq 0} M_k(\Gamma)$ becomes a $\mathbb{Z}$-graded commutative $\mathbb{C}$-algebra.

[1] The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by fractional linear transformations extends continuously to $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, preserving each piece of this union and acting transitively on the latter.

Definition 1.2. *A modular form f of level Γ which vanishes at all cusps of Γ is called a* **cusp form**. *The set of cusp forms of weight k and level Γ forms a subspace $S_k(\Gamma)$ of $M_k(\Gamma)$.*

We are principally interested in modular forms for the family of congruence subgroups $\Gamma_0(N),\ N \in \mathbb{Z}_{\geq 1}$ defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod N \right\}.$$

If f is a cusp form for $\Gamma_0(N)$, the vanishing condition at ∞ (together with the fact that the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ belongs to $\Gamma_0(N)$) implies that f has a Fourier expansion of the shape

$$f(z) = \sum_{n=1}^{\infty} a_n q^n \quad \text{where } q = e^{2\pi i z}.$$

Notice that whenever $M \in \mathbb{Z}_{\geq 1}$ divides N we have $\Gamma_0(N) \subseteq \Gamma_0(M)$. Consequently, we have an inclusion $M_k(\Gamma_0(M)) \hookrightarrow M_k(\Gamma_0(N)$. It will turn out to be important to distinguish modular forms (especially cuspforms) which truly live at level $\Gamma_0(N)$ from those which appear as flotsam from lower levels.

Definition 1.3. *A cusp form of level $\Gamma_0(N)$ which is also a cusp form for $\Gamma_0(M)$ for some M dividing N is called an* **oldform**.

Remark: The oldforms generate a subspace of the space of cusp forms. We shall refer to this subspace as the **oldspace** of $S_k(\Gamma_0(N))$ and denote it by $S_K^{\text{old}}(\Gamma_0(N))$.

There exists a certain inner product on $S_k(\Gamma_0(N))$ called the *Petersson inner product.*[2] The orthogonal complement of $S_k^{\text{old}}(\Gamma_0(N))$ with respect to the Petersson inner product is called the **newspace** of $S_k(\Gamma_0(N))$ and is denoted by $S_k^{\text{new}}(\Gamma_0(N))$.

Central to the classical theory of modular forms are certain families of weight and level preserving linear operators collectively known as *Hecke-operators.* We shall define them via their action on Fourier expansions.

Definition 1.4. *Fix positive integers k and N. For each prime number p the* **Hecke-operator** *T_p on $M_k(\Gamma_0(N))$ is defined by the formula*

$$T_p\Big(\sum_{n\geq 0} a_n q^n\Big) = \begin{cases} \sum_{n\geq 0} a_{np} q^n + p^{k-1} \sum_{n \geq 0, p \mid n} a_{n/p} q^n & \textit{if } p \nmid N, \\ \sum_{n\geq 0} a_{np} q^n & \textit{if } p \mid N. \end{cases}$$

A straightforward computation shows that the family of prime Hecke operators is commutative, ie. that if p and l are primes then $T_p T_l = T_l T_p$. The remaining operators are defined recursively according to the rules

- T_1 is the identity operator;
- if $\gcd(m, n) = 1$ then $T_{mn} := T_m T_n$;

[2] The one ad only thing we need to know about the Petersson inner product is that it exists. See [Van Der Geer, §5] for its definition and basic properties.

- For $r \geq 2, T_{p^r} := T_p T_{p^{r-1}} - p^{k-1} T_{p^{r-2}}$.

The algebra generated by the full set $\{T_n\}_{n \in \mathbb{N}}$ of Hecke operators is called the **Hecke algebra**. For each n and k the operator T_n preserves both the space $S_k(\Gamma_0(N))$ and its newspace. Furthermore, it can be shown that each T_n is self adjoint on $S_k^{\text{new}}(\Gamma_0(N))$ with respect to the Petersson inner product, and it follows (from the spectral theorem for commuting families of self adjoint operators) that $S_k^{\text{new}}(\Gamma_0(N))$ admits a basis of simultaneous eigenvectors for this family.

Definition 1.5. *A* **Hecke-eigenform** *is a modular form that is a simultaneous eigenvector for the full family $\{T_n\}_{n \in \mathbb{N}}$ of Hecke operators.*

We remark that if $f = \sum_{n \geq 1} a_n q^n$ is an eigenvector of T_n with eigenvalue λ_n then a consideration of the coefficient of q in $T_n f$ leads to the identity $a_n = \lambda_n a_1$. Two immediate condquences are

1. if $f = \sum_{n \geq 1} a_n q^n$ is a simultaneous eigenvector of all the Hecke operators then $a_1 \neq 0$;
2. if we normalise f so that $a_1 = 1$ then the Fourier coefficients of f are identical with its Hecke eigenvalues.

Definition 1.6. *A* **newform** *is a Hecke-eigenform in $S_k^{new}(\Gamma_0(N))$ with the normalisation $a_1 = 1$.*

1.2 Elliptic curves

Let K be a field and consider a cubic plane curve E over K (ie. the zero locus in $\mathbb{P}^2(\mathbb{C})$ of a polynomial in $K[X, Y, Z]$ of homogeneous degree 3) defined by an equation of the form

$$E : Y^2 + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3.$$

Such an equation is called a **Weierstraß equation**. Note that such a curve always contains the k-rational point $[0 : 1 : 0]$ ie. the point at infinity with respect to the affine patch $(x, y) \mapsto [x : y : 1]$. If $\text{char}(K) \neq 2, 3$ then it is always possible to make change of projective coordinates that puts the Wierstraß equation in the form

$$E : Y^2 Z + = X^3 + AXZ^2 + BZ^3.$$

By an **elliptic curve** we mean a curve E of the above type such that the **discriminant**

$$\Delta(E) = -16(4A^3 + 27B^2)$$

of E does not vanish. If there exists a change of projective coordinates such that E is defined by a polynomial with coefficients in some subfield K' of K then one may equally say that E is an elliptic curve over K'.

Let us now specialise to the case $K = \mathbb{Q}$. If E is an elliptic curve over $\mathbb{Q}$ then it is a more or less trivial fact that (with respect to an appropriate set of coordinates on $\mathbb{P}^2(\mathbb{Q})$) E can be defined by an *integral* Weierstraß equation, ie.

$$E : Y^2 Z = X^3 + AXZ^2 + BZ^3 \quad \text{where } A, B \in \mathbb{Z}.$$

For any prime number $p \neq 2, 3$, the **reduction** of E at p is the cubic plane curve over the finite field $\mathbb{F}_p$ defined by reducing A and B mod p. [3] This will be an elliptic curve over $\mathbb{F}_p$ so long as p does not divide the discriminant $\Delta(E)$ of E.

Certain heuristic arguments (which we forego reproducing) lead one to the following naïve estimate of the number of points on a reduced curve: the reduction mod p of a generic Weierstraß equation should have $p + 1$ solutions in $\mathbb{P}^2(\mathbb{F}_p)$.

1.3 The (elliptic) modularity theorem

We are now (almost[4]) equipped to give a precise statement of the modularity theorem.

Theorem 1. (Taylor-Wiles, Taylor-Breuil-Conrad-Diamond) *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E. Define a sequence $(a_n)_{n\in\mathbb{Z}_{\geq 1}}$ according to the recipe*

1. $a_1 := 1$;
2. *for p a prime number set $a_p := p + 1 - \#E(\mathbb{F}_p)$;*
3. *for $r \geq 2$ set $a_{p^r} := a_p a_{p^{r-1}} - p^{k-1} a_{p^{r-2}}$*
4. *for $gcd(m, n) = 1$ set $a_{mn} := a_m a_n$.*

Then $\sum_{n\geq 1} a_n q^n$ is the Fourier expansion of a newform of weight 2 and level $\Gamma_0(N_E)$.

□

1.4 A Mission Statement and a Roadmap.

The relationship between elliptic curves and modular forms established by the stunning theorem 1 is an instance of a phenomenon called **modularity**. The first goal of this thesis is to explain what modular forms and elliptic curves are and where they come from in a way that makes the modularity theorem (marginally!) less shocking. The second goal is to instil in the reader some degree of optimism (however guarded) that – in light of the theorem 1 – a kind of "generalised" modularity theorem (or perhaps several theorems) might actually exist. We do this by introducing natural generalisations of modular forms and elliptic curves and arguing that the deep connections that exist between elliptic curves and modular forms exist also between their respective generalisations.

In §2 we introduce abelian varieties as higher dimensional analogues of elliptic curves, first over general fields and then over the complex numbers. In §3 we begin by establishing a connection between abelian varieties and symplectic groups and then show how to interpret modular forms as line bundles on symmetric spaces for these same groups. §4 is devoted to developing a group theoretical definition of Hecke algebras and explaining the central role played by of Hecke eigenforms with respect to any (real or putative) modularity phenomenon. In §5 we discuss some

[3] The issue with 2 and 3 is the same one already alluded to. In this case one considers a reduction mod p of a general Weierstraßequation for E.

[4] The definition of the conductor N_E of an elliptic curve E is rather non-elementary. We defer the definition to §2.5

of the inherent difficulties in formulating a coherent “generalised modularity conjecture” for Abelian varieties, and give an all too brief survey of known (or merely observed and dearly hoped for) instances of modularity phenomena beyond theorem 1.

At the end of the text can be found a trio of appendices in which we cover some necessary theory which did not find a comfortable home in the body of the text.

2 Abelian varieties

Throughout this section K will denote a field.

Definition 2.1. *An* **algebraic group scheme** *over a commutative ring R is a R-scheme $G \to Spec(R)$ with* **(i)** *a section $e : Spec(R) \to G$,* **(ii)** *an R-morphism $\mu : G \times_R G \to G$, and* **(iii)** *an R-morphism $-1 : G \to G$ such that the following diagrams*

$$\begin{tikzcd}
& G \times_R G \times_R G \arrow[dl, "\mu \times 1"'] \arrow[dr, "1 \times \mu"] & \\
G \times_R G \arrow[dr, "\mu"'] & & G \times_R G \arrow[dl, "\mu"] \\
& G &
\end{tikzcd}$$

$$\begin{tikzcd}
& G \arrow[dl, "1 \times -1"'] \arrow[d] \arrow[dr, "-1 \times 1"] & \\
G \times_R G \arrow[dr, "\mu"'] & Spec(R) \arrow[d, "e"'] & G \times_R G \arrow[dl, "\mu"] \\
& G &
\end{tikzcd}$$

commute and such that for each R-algebra A the set $G(A)$ of A-points of G is a group with multiplication $G(A) \times G(A) \to G(A)$, $(g,h) \mapsto gh$ and inversion $G(A) \to G(A), g \mapsto g^{-1}$ and identity induced by $\mu, -1$ and e respectively.

Examples 2.1.

Let R be a commutative ring.

1. The **multiplicative group scheme** is the $\mathbb{Z}$-scheme $\mathbb{G}_m$ whose set of R points is
$$\mathbb{G}_m(R) = R^\times$$
ie. the multiplicative group of units in R. It is easy to see that $R^\times$ is in bijection with the set of ring homomorphisms $\mathrm{Hom}(\mathbb{Z}[t,t^{-1}], R)$ since **(i)** any homomorphism must send t to a unit in R, and conversely **(ii)** every unit $u \in R$ determines a unique homomorphism $\varphi_u : \mathbb{Z}[t,t^{-1}] \to R$ with $\varphi_u(t) = u$. Thus $\mathbb{G}_m = \mathrm{Spec}(\mathbb{Z}[t,t^{-1}])$ ie. $\mathbb{G}_m$ is affine and we may identify the inversion and multiplication morphisms of $\mathbb{G}_m$ with homomorphisms in the category of rings. The inversion morphism $-1 : \mathbb{Z}[t,t^{-1}] \to \mathbb{Z}[t,t^{-1}]$ is the homomorphism interchanging t and t^{-1}, and the multiplication morphism μ is the ring homomorphism
$$\begin{array}{rcl} \mu : \mathbb{Z}[t,t^{-1}] & \to & \mathbb{Z}[t,t^{-1}] \otimes_{\mathbb{Z}} \mathbb{Z}[t,t^{-1}] \\ t & \mapsto & t \otimes t. \end{array}$$
To see why, note that **(i)** $\mathrm{Spec}(R \otimes_{\mathbb{Z}} S) = \mathrm{Spec}(R) \times_{\mathbb{Z}} \mathrm{Spec}(S)$ for all commutative rings R and S and that **(ii)** each pair of homomorphisms $\varphi_a, \varphi_b \in \mathrm{Hom}(\mathbb{Z}[t,t^{-1}], R)$ induces a homomorphism $\varphi_a \otimes \varphi_b \in \mathrm{Hom}(\mathbb{Z}[t,t^{-1}] \otimes_{\mathbb{Z}} \mathbb{Z}[t,t^{-1}], R)$ such that $\varphi_{ab} = (\varphi_a \otimes \varphi_b) \circ \mu$.

2. The **general linear group scheme** (of degree n) is the $\mathbb{Z}$-scheme GL_n whose set of R-points is the group of invertible n by n matrices over R:

$$\mathrm{GL}_n(R) = \{X \in \mathrm{Mat}_n(R) \mid \det X \in R^\times\}.$$

It turns out that GL_n is affine: explicitly we have $\mathrm{GL}_n = \mathrm{Spec}\big(\mathcal{O}(\mathrm{GL}_n)\big)$ where

$$\mathcal{O}(\mathrm{GL}_n) := \mathbb{Z}[\{x_{ij}\}_{1\leq 1,j\leq n}, y]/\langle \det\big(x_{ij}\big)y - 1\rangle$$

and where det is the familiar determinant mapping thought of as a polynomial function of n^2 variables. The multiplication morphism is

$$\begin{array}{rcl} \mu : \mathcal{O}(\mathrm{GL}_n) & \to & \mathcal{O}(\mathrm{GL}_n) \otimes_{\mathbb{Z}} \mathcal{O}(\mathrm{GL}_n), \\ x_{ij} & \mapsto & \displaystyle\sum_{k=1}^{n} x_{ik} \otimes x_{kj}, \\ y & \mapsto & y \otimes y. \end{array}$$

To see why, suppose that for each R-point $S \in \mathrm{GL}_n(R)$ we let $\varphi_S : \mathcal{O}(\mathrm{GL}_n) \to R$ be the corresponding homomorphism in the category of rings. Then given a pair of R points S, T there is an induced homomorphism

$$\varphi_S \otimes_{\mathbb{Z}} \varphi_T : \mathcal{O}(\mathrm{GL}_n) \otimes_{\mathbb{Z}} \mathcal{O}(\mathrm{GL}_n) \to R$$

which is defined on "simple" tensors by

$$\varphi_S \otimes_{\mathbb{Z}} \varphi_T(f \otimes g) = \varphi_S(f)\varphi_T(g).$$

It is now easy to check that $\varphi_{ST} = (\varphi_S \otimes_{\mathbb{Z}} \varphi_T) \circ \mu$. With enough patience, the inversion morphism can be written down as an explicit polynomial function.[5]

3. The **additive group scheme** $\mathbb{G}_a$ over $\mathbb{Z}$ represents the forgetful functor from the category of rings to the category of abelian groups. It can be realised as a subgroup scheme[6] of GL_2 by declaring its set of R points to be

$$\mathbb{G}_a(R) = \left\{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \mid r \in R \right\}.$$

Definition 2.2. *An* **algebraic group** *(or* **group variety***) is a group scheme G over a field K such that G is also a smooth variety over K.*

Remark: Each of the above group schemes over $\mathbb{Z}$ becomes an algebraic group over K after base change to K. Each is also an example of a **linear algebraic group** ie. a subgroup variety of GL_n for some n. In fact it is a theorem that every **affine** algebraic group is linear.[7]

Definition 2.3. *An* **abelian variety** *is a connected and projective algebraic group.*

[5] It is easy to see that inversion morphism really is polynomial: for instance, invoke Cramer's rule and the polynomiality of the determinant map.

[6] A **subgroup scheme** of a group scheme $(G, \mu, (\cdot)^{-1})$ is a subscheme $\iota : X \hookrightarrow G$ such that $(X, \iota^*\mu, \iota^*(\cdot)^{-1})$ is itself a group scheme.

[7] This applies to the additive group variety $\mathbb{G}_a \times_{\mathbb{Z}} \mathrm{Spec}(K)$ over K since it is a subvariety of the affine variety $\mathrm{GL}_2 \times_{\mathbb{Z}} \mathrm{Spec}(K)$ and thus itself affine.

Remark: Despite the fact that abelian varieties are groups (or at least are group-like[8]), the adjective “abelian” has (*a priori*) nothing at all to do with abelian groups. The adjective instead indicates a historical connection to the classical theory of *abelian integrals/functions*. It would take a monumental effort of will to maintain this semantic distinction in the face of the following theorem.

Theorem 2. *The group law on an abelian variety is commutative. That is, if A is an abelian variety over a field K then $A(R)$ is an abelian group for every commutative K-algebra R.*

Proof. See [Milne, §2, corollary 2.4].

□

A morphism $\varphi : A \to B$ of abelian varieties over K is a morphism of K-varieties which induces a group homomorphism $A(R) \to B(R)$ for all K-algebras R.

Definition 2.4. *An* **isogeny** *is a morphism of abelian varieties with finite kernel.*

Example 2.1.

Let A be an abelian variety over K. For all natural numbers N the **multiplication by** N isogeny is the composition

$$A \to \underbrace{A \times_K A \times_K \ldots \times_K A}_{N \text{ times}} \to A$$

where the first arrow is the diagonal mapping $x \mapsto (x, \ldots, x)$ and the second arrow consists of an N-fold iteration of the multiplication morphism $\mu : A \times_K A \to A$.[9]

Proposition 2.1. *If $\varphi : A \to B$ is an isogeny then there exists an isogeny $\varphi^\wedge : B \to A$.*

Proof. See [Rosen, §2, page 81].

□

Corollary 2.1. *The relation “there exists an isogeny from A to B” is an equivalence relation on the set of abelian varieties over a field K.*

The following theorem tells us that under mild assumptions on the field K one can (almost!) understand the whole category of algebraic groups over K by understanding two *a priori* special species of algebraic groups over K.

Theorem 3. *(Chevalley's structure theorem) Let K be a perfect field[10] and let G be an algebraic group over K. Then there exists a canonical exact sequence of algebraic groups*

$$1 \to H \to G \to A \to 1$$

where H is a closed affine algebraic subgroup of G and where A is an abelian variety.

[8] Abelian varietie over K are precisely the (connected) **group objects** in the category of projective varieties over K.

[9] We can afford to be vague about the precise definition of the latter map since μ is associative.

[10] A field K is perfect if either **(i)** $\mathrm{char}(K) = 0$ or else **(ii)** $\mathrm{char}(K) = p$ and $x \mapsto x^p$ is an automorphism of K.

2.1 Elliptic curves

Let K be an algebraically closed field of characteristic different from 2 or 3. In the introduction we defined an elliptic curve E over K as the solution set in $\mathbb{P}^2(K)$ of a non-singular Weierstraß equation, eg. a homogeneous cubic equation of the form

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3$$

with discriminant $\Delta(E) = -16(4A^3 + 27B^2) \neq 0$. Our immediate aim is to redefine elliptic curves in the following way:

Definition 2.5. *An elliptic curve is an abelian variety of dimension one.*

We begin with some necessary definitions.

Definition 2.6. *Let C be a smooth algebraic curve over an algebraically closed field K. The group $Div(C)$ of* **divisors** *on C is the free abelian group on the K-points of C. Thus an element D of $Div(C)$ is a formal $D = \sum_{P \in C(K)} a_P P$ where each a_P is an integer and $a_P = 0$ for all but finitely many P. The* **degree** *of $D = \sum_{P \in C(K)} a_P P$ is $deg(D) := \sum_{P \in C(K)} a_P$. A divisor D is said to be* **effective** *if $a_P \geq 0$ for all $P \in C(K)$.*

Let $K(C)$ be the **function field** of C ie. the stalk of the structure sheaf $\mathcal{O}_C$ at the generic point. If $P \in C(K)$ and x is a coordinate function in a neighbourhood of P with $x(P) = 0$ then every $f \in K(C)$ is (locally) of the form $f(x) = p(x)/q(x)$ where $p, q \in K[x]$ are polynomials of the same degree. Without loss of generality, p and q are relatively prime in $K[X]$, under which assumption the representation $f = p/q$ is (for all intents and purposes) unique with respect to the coordinate function x.

Definition 2.7. *Let P, x and $f = p(x)/q(x)$ be as above.*

1. *One says that f has a* **zero of order** n **at** P *if $q(x) = x^n r(x)$ where $r(x) \neq 0$.*

2. *One says that f has a* **pole of order** n **at** P *if $p(x) = x^n s(x)$ where $s(x) \neq 0$.*

Using the same definitions, one may associate a divisor $D(\omega)$ to each differential $\omega \in \Omega^1_C$.[11]

Definition 2.8. *A* **principal divisor** *on C is a divisor of the form*

$$D(f) := \sum_{P \in C(K)} ord_P(f)P$$

where $f \in K(C)$ and where

$$ord_P(f) := \begin{cases} n, & \text{if } f \text{ has a zero of order } n \text{ at } P; \\ -n, & \text{if } f \text{ has a pole of order } n \text{ at } P; \\ 0, & \text{otherwise.} \end{cases}$$

The subgroup of $Div(C)$ of principal divisors is denoted $Div_0(C)$.

[11] In the stalk of Ω^1_C at $P \in C(K)$ and x as above, ω has a unique representation $\omega = f(x)dx$ in a neighbourhood of p and one defines $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$. This definition is independent of the choice of coordinate function x.

Remark: Since K is algebraically closed and every $f \in K(C)$ is locally p/q for coprime polynomials p, q of equal degree it follows that $\deg(D(f)) = 0$.

Definition 2.9. *The quotient $Div(C)/Div_0(C)$ of the divisor group of C by its subgroup of principal divisors is called the* **Picard group** *$Pic(C)$ of C. $Pic^0(C)$ denotes the subgroup of the $Pic(C)$ consisting of divisor classes of degree 0.*

Remark: One can show that $D(\omega) - D(\theta)$ is principal for all $\omega, \theta \in \Omega^1_C$ and so there is a unique class in $\mathrm{Pic}^0(C)$ containing the divisors of all differential 1-forms on C. We will denote this divisor class by $\mathcal{K}_C$ and refer to it as the **canonical divisor** of C.

Definition 2.10. *The* **genus** *of an algebraic curve C is the dimension of the vector space $H^1(C, \Omega^1_C)$.*

For $D = \sum_{P \in C(K)} a_P P \in \mathrm{Div}(C)$ we define a vector space $L(D)$ over K as follows:

$$L(D) := \{f \in K(C) \mid D + D(f) \text{ is effective}\} \cup \{0\}.$$

Thus a (non-zero) element of $L(D)$ is a function $f \in K(C)$ such that

- if $a_P < 0$ then f has a zero of order $\geq a_P$ at P;
- if $a_P \geq 0$ then f has a pole of order $\leq a_P$ at P.

It is easy to see that if $D - D'$ is principal then $L(D)$ and $L(D')$ are isomorphic. Indeed, if $D - D' = D(g)$ for some $g \in K(C)$ then $f \mapsto gf$ is a K-linear isomorphism $L(D') \xrightarrow{\sim} L(D)$. Additionally, since every non constant $f \in K(C)$ has a pole it follows that $L(-D) = 0$ whenever D is an effective divisor.

Theorem 4. *(Riemann-Roch theorem) Let K be an algebraically closed field and let C be a smooth algebraic curve of genus g over K . Let $\mathcal{K}_C$ be the canonical divisor of E. Then for all divisors D on C,*

$$\dim_K L(D) - \dim_K L(\mathcal{K}_C - D) = deg(D) - g + 1.$$

Before we move on we pause to record the following fact.

Proposition 2.2. *A smooth algebraic curve C of genus 1 possesses a differential 1-form without zeroes or poles. Consequently, the canonical divisor $\mathcal{K}_C$ is trivial.*

Proof. See [Husemöller, §2, page 68.]

□

Let E be a smooth algebraic curve of genus 1 over an algebraically closed field K and fix a point $\mathcal{O} \in E(K)$. Since $D(\mathcal{K}_E) = 0$ in $\mathrm{Pic}^0(E)$, the Riemann-Roch theorem for divisors D on E simplifies to

$$\dim_K L(D) - \dim_K L(-D) = \deg(D).$$

In the case that D is effective this simplifies yet further to $\dim_K L(D) = \deg(D)$.

Consider now the sequence of effective divisors $\{n\mathcal{O} \mid n \in \mathbb{N}\}$.

1. By construction, $L(n\mathcal{O})$ is a subspace of $L((n+1)\mathcal{O})$ for all $n \in \mathbb{N}$.

2. Since $\dim_K L(\mathcal{O}) = 1$ and we know constant functions $K \subseteq K(E)$ certainly belong to $L(\mathcal{O})$ we conclude that $L(\mathcal{O}) = K$. We take $1 \in K$ as our generator for this space.

3. Since $\dim_K L(2\mathcal{O}) = 2$ we may conclude that there exists a one dimensional space of functions on E with a double pole at $\mathcal{O}$ and no other poles on E. Let x be a generator for this space of functions.

4. Similarly, we conclude that there exists a function y on C with a triple pole at $\mathcal{O}$ and no poles elsewhere on E.

Starting with the functions $1, x, y$ we may can construct seven elements of $L(6\mathcal{O})$, namely $1, x, y, x^2, xy, x^3$ and y^2. As the space $L(6\mathcal{O})$ is only six dimensional we conclude that there exists an equation of linear dependence over K between these seven functions. We arrive at the punchline: said equation of linear dependence is (once homogenised to a cubic polynomial with a third varible z) a Weierstraß equation[12] satisfied by the coordinate functions x and y, and the map

$$E(K) \to \mathbb{P}^2(K), \quad P \mapsto [x(P) : y(p) : 1]$$

is an embedding of E into $\mathbb{P}^2(K)$ as the zero locus of that equation. Thus every datum $(E, \mathcal{O})$ with E a smooth algebraic curve over K of genus 1 and $\mathcal{O} \in E(K)$ a choice of point in E determines an elliptic curve over K.

Proposition 2.3. *The function*

$$\begin{array}{rcl} E(K) & \to & Pic^0(E), \\ P & \mapsto & P - \mathcal{O} \end{array}$$

is a bijection.

Proof. A general degree zero divisor on E is of the form

$$D = \sum_{i=1}^{n} P_i - Q_i$$

where $P_i \neq Q_j$ for all i, j but where we allow for the possibility that $P_i = P_j$ and/or $Q_i = Q_j$ without restriction. For $n = 1$, Riemann-Roch tells us that a function in $K(E)$ can never have exactly one pole (counted with multiplicity), so

$$\dim_K L(P_1 - Q_1 + \mathcal{O}) = \deg(P_1 - Q_1 + \mathcal{O}) = 1$$

[12] That the discriminant of this cubic equation is non-zero follows from the smoothness of E. Indeed, recall that when the characteristic of K is neither 2 nor 3 then any cubic equation in two variables over K can be put in the form $y^2 = x^3 + Ax + B$. The algebraic plane curve described by this equation is smooth so long as the partial derivatives (with respect to the coordinates x and y) of this equation never simultaneously vanish on the curve. By direct computation the partial derivative with respect to y vanishes if and only if $y = 0$ whereas the partial derivative with respect to x vanishes if and only if $x = \pm\sqrt{-A/3}$. By evaluating the defining equation of the curve at the potentially bad points $(x, y) = (\pm\sqrt{-A/3}, 0)$ we conclude that the curve is singular precisely when $4A^3 + 27B^2 = 0$ ie. precisely when the discriminant $-16(4A^3 + 27B^2)$ of the equation vanishes.

Thus (up to scaling) there exists a unique $f \in K(E)$ whose divisor is $D(f) = Q_1 - P_1 - \mathcal{O} + R_1$ for a unique $R_1 \in E(K)$ which means that $P_1 - Q_1$ is equivalent to $R_1 - \mathcal{O}$ in the Picard group. When $n = 2$, an entirely similar argument implies that there exists a function $g \in K(E)$ (unique up to scaling) whose divisor is $D(g) = S + Q_1 - P_1 - P_2$ for a (unique) point $S \in E(K)$ and we are back in the case $n = 1$. By induction we find that $E(K)$ surjects onto $\mathrm{Pic}^0(E)$. A final application of Riemann-Roch shows us that no function in $K(E)$ can have a divisor of the form $P - Q$ for $P, Q \in E(K)$, whence injectivity (and thus bijectivity) follows.

□

This bijection induces an abelian group structure on $E(K)$ with identity element $\mathcal{O}$, eg. for $P, Q \in E(K)$ we define $P + Q$ to be the unique $R \in E(K)$ such that $P + Q - 2\mathcal{O} = R - \mathcal{O}$ in $\mathrm{Pic}^0(E)$. One could be forgiven for doubting that this group law is at all compatible with the geometry of E. Such scepticism turns out to be spectacularly unfounded.

Proposition 2.4. *$P + Q + R = \mathcal{O}$ in $E(K)$ if and only if the points P, Q and R are collinear in $\mathbb{P}^2(K)$.*

Proof. For simplicity's sake we will assume that none of P, Q or R is equal to $\mathcal{O}$.[13] Suppose $P + Q + R = \mathcal{O}$. From the definition of the group law on $E(K)$ this means that $P + Q + R - 3\mathcal{O} = D(f)$ for some $f \in K(C)$. Such an f belongs to $L(3\mathcal{O})$ and since the coordinate functions x, y were chosen so that $1, x, y$ would be a basis for $L(3\mathcal{O})$ we are able to write $f = a + bx + cy$ for some $a, b, c \in K$. But since $f(P) = f(Q) = f(R) = 0$ this means that all three points lie on the line $\{[Z : X : Y] \mid aZ + bX + cY = 0\}$ in $\mathbb{P}^2(K)$. Reversing this argument shows that $P + Q + R = \mathcal{O}$ whenever P, Q and R are colinear in $\mathbb{P}^2(K)$.

□

Corollary 2.2. *For every $P \in E(K)$, $-P$ is the remaining point of intersection between $E(K)$ and the line in $\mathbb{P}^2(K)$ through P and $\mathcal{O}$.*

Proof. Recall **Bezout's theorem**: a pair of curves in $\mathbb{P}^2(K)$ of respective degree n and m intersect in precisely nm points (counted with muliplicity). Thus there is a unique third point (counted with multiplicity) in the intersection between $E(K)$ and the line through P and $\mathcal{O}$. If we call this point R then by the preceding proposition we have $P + R = P + R + \mathcal{O} = \mathcal{O}$ (recall that $\mathcal{O}$ is the identity element).

□

We thus have a purely geometric way to define the sum of any two points $P, Q \in E(K)$: if R is the third intersection point of $E(K)$ with the line through P and Q then $P + Q$ is the third point of intersection of $E(K)$ with the line through R and $\mathcal{O}$. In light of this description it is (relatively) easy to see that if $P = [p_1 : p_2 : p_3]$ and $Q = [q_1 : q_2 : q_3]$ then $P + Q = [f_1 : f_2 : f_3]$ where each f_i is a rational function of the p_i and q_j with coefficients in K. Similarly, the involution of $E(K)$ taking each point to its inverse with respect to the group law is also given by rational functions. We have just proved

Theorem 5. *An elliptic curve $(E, \mathcal{O})$ is an algebraic group.*

[13] In the case that one or more of P, Q, R is $\mathcal{O}$ the following proof must be adapted accordingly. This is tedious rather than difficult and so we omit these cases.

Since an elliptic curve is also a one dimensional projective variety we are now entitled to adopt the following defintion:

Definition 2.11. *An elliptic curve is an abelian variety of dimension one.*

2.2 Abelian varieties over $\mathbb{C}$

When $K = \mathbb{C}$ there is an obvious, naïve method – based on the rough intuition that a compact complex manifold should be (more or less) the same thing as a complex projective variety – for producing (potentially!) abelian varieties over $\mathbb{C}$,

Definition 2.12. *Let V be a g-dimensional complex vector space. A* **lattice** *in V is a free $\mathbb{Z}$-submodule Λ in V of rank $2g$ such that the canonical inclusion $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \hookrightarrow V$ is an isomorphism of vector spaces over $\mathbb{R}$.*

Definition 2.13. *A* **complex torus** *of dimension g is an orbit space of the form V/Λ where V is a complex vector space and Λ is a lattice in V. A* **morphism** *between complex tori $V/\Lambda, W/\Lambda'$ is a $\mathbb{C}$-linear mapping $T : V \to W$ such that $T(\Lambda) \subseteq \Lambda'$. T is an isomorphism if $\dim V = \dim W$ and $T(\Lambda) = \Lambda'$.*

Every complex torus $X = V/\Lambda$ inherits a complex structure and an abelian group law $\mu(z, w) = z + w \mod \Lambda$ from V and is thus a compact commutative complex Lie group. However, it is not the case that every complex torus is an abelian variety. Before we can hope to use complex tori to study abelian varieties we must first solve the following recognition problem: for which lattices $\Lambda \subseteq V$ is V/Λ a projective (and thus also an abelian) variety?

The essential insight is this: to say that $X = V/\Lambda$ is projective is to say that there exists an embedding $\eta : X \hookrightarrow \mathbb{P}^n$ for some n. There exists a certain line bundle[14] $\mathcal{O}(1)$ on $\mathbb{P}^n$ that when pulled back along the embedding η induces what is known as a **very ample line bundle** on X. This line bundle can be pulled futher back along the quotient mapping $V \to V/\Lambda$ to product a rather special line bundle on V satisfying a rich set of symmetries with respect to the action of Λ. We shall see that the existence (or non-existence) of an embedding η is determined by the existence (or non-existence) of a certain piece of linear algebraic data attached to the pair (V, Λ): a **polarization**.

2.3 Line bundles on orbit spaces

Before we specialise to the case of complex tori, we will cover some of the general theory of line bundles on orbit spaces .

Let V be a complex manifold and let G be a group acting on V by biholomorphisms $V \xrightarrow{\sim} V$ in such a way that the quotient $X := \Gamma\backslash V$ is once again a complex manifold.[15] Suppose we are given a holomorphic (resp. meromorphic) line bundle

[14] See appendix B for a general discussion of line bundles on projective spaces.

[15] For expositional reasons we will assume that the action of G is free and properly discontinuous. This assumption is not strictly necessary: group actions on V with discrete orbits and finite stabilisers can be accommodated at the expositional cost of introducing orbifolds. This cost being altogether too steep for the present document (to say nothing of its author!), we beg the reader's indulgence in allowing us to assert rather more than we are prepared to prove.

$p : \mathscr{L} \to X$. Our immediate aim is to show that holomorphic (resp. meromorphic) sections of $p : \mathcal{L} \to X$ may be identified with holomorphic (resp. meromorphic) functions on V satisfying certain explicit functional equations which are themselves jointly determined by the transition functions of the bundle and the action of G.

We briefly recall the definition of the canonical quotient atlas on $X = G\backslash V$. Let $\pi : V \to X$ be the (holomorphic) quotient map. For $x \in V$, let $[x] = \pi(x)$, let Gx denote the G-orbit of x and let $\mathcal{S}_x$ be the set of all (U, φ_U) in the holomorphic atlas of V such that U is an open connected neighbourhood of x on which the restriction $\pi|_U : U \to \pi(U)$ is a biholomorphism. Then an explicit basis of open neighbourhoods of $[x]$ in X is

$$\mathcal{S}_{[x]} = \{\pi(U) \mid U \in \mathcal{S}_y \text{ for some } y \in Gx.\}$$

For each $U \in \mathcal{S}_{[x]}$, $\pi^{-1}(U)$ is by construction a disjoint union $\bigsqcup_{g\in G} U_g$ with the following properties:

1. $U_{gh} = gU_h$ for all $g, h \in G$. In other words, $\pi^{-1}U$ is the orbit of a single connected component U_1 (chosen arbitrarily) where $1 \in G$ is the identity element.

2. For all $g \in G$, π restricts to a biholomorphism $\pi|_{U_g} : U_g \xrightarrow{\sim} U$.

The neighbourhood atlas of $[x]$ is the set of all pairs (U, f) where $U \in \mathcal{S}_{[x]}$ and where f is a composition

$$U \xrightarrow{\pi|_{U_g}^{-1}} U_g \xrightarrow{F} \mathbb{C}^n$$

with F a biholomorphic map between U_g and an open subset of $\mathbb{C}^n$.

The quotient map $\pi : V \to X$ induces a holomorphic line bundle $\pi^*p : \mathscr{L}_V \to V$ whose fibre above $z \in V$ is canonically identified with fibre of $p : \mathscr{L} \to X$ above $\pi(z) \in X$. This is the (categorical) fibre product of p and π, ie. the bundle for which the pullback square

$$\begin{tikzcd}
\mathscr{L}_V \arrow[r] \arrow[d, "\pi^*p"'] & \mathscr{L} \arrow[d, "p"] \\
V \arrow[r, "\pi"'] & X
\end{tikzcd}$$

is universal.

For every open set $U \in X$ there is an induced homomorphism[16]

$$\begin{array}{rcl} \pi^* : \mathscr{L}(U) & \to & \mathscr{L}_V(\pi^{-1}U), \\ s & \mapsto & s \circ \pi \end{array}$$

where $\mathscr{L}(U)$ (resp. $\mathscr{L}_V(\pi^{-1}U)$) is the vector space of sections of $p : \mathscr{L} \to X$ over U (resp. sections of $\pi^*p : \mathscr{L}_V \to V$ over $\pi^{-1}U$).

Let us now attempt to characterise the image of such a homomorphism. Let $U \subset X$ be such that

[16] This can be promoted to a homomorphism of $\mathcal{O}_X$ modules where $\mathcal{O}_X$ is the sheaf of holomorphic functions on X (mapping to $\mathcal{O}_V$ via pullback along π).

1. $\pi^{-1}U$ is a disjoint union $\bigsqcup_{g\in G} U_g$ as previously described;
2. The bundle $p : \mathscr{L} \to X$ is trivialisable over U.

Since $\pi^{-1}U$ is a disjoint union, a holomorphic section of $\mathscr{L}_V$ over $\pi^{-1}U$ is the same thing as a family of holomorphic sections

$$\{s_g \in \mathscr{L}_V(U_g)\}_{g\in G}.$$

For each g let $\varphi_g : p^{-1}U_g \xrightarrow{\sim} U_g \times \mathbb{C}$ be a trivialisation and identify s_g with a holomorphic function $f_g : U_g \to \mathbb{C}$ like so:

$$\varphi_g \circ s_g(z) = \big(z, f_g(z)\big).$$

Notice that we may interpret $\{\varphi_g\}_{g\in G}$ as a family of trivialisations[17] of $p : \mathscr{L} \to X$ over U. Indeed, in order to write down the the transition maps between the various trivialisations quite explicitly one need only observe that there exists a unique nowhere vanishing holomorphic function $j_g : \bigsqcup_{h\in G} U_h \to \mathbb{C}^\times$ such that the function

$$\begin{array}{rcl} T_g : \displaystyle\bigsqcup_{h\in G} U_h \times \mathbb{C} & \to & \displaystyle\bigsqcup_{gh\in G} U_{gh} \times \mathbb{C}, \\ (z,w) & \mapsto & (gz, j_g(z)w) \end{array}$$

makes the following diagram commute:

$$\begin{tikzcd} U_h \times \mathbb{C} \arrow[rr, "T_g"] & & U_{gh} \times \mathbb{C} \\ & p^{-1}(U) \arrow[ul, "\varphi_h"] \arrow[ur, "\varphi_{gh}"'] & \end{tikzcd}$$

To say that s is in the image of $\pi^* : \mathscr{L}(U) \to \mathscr{L}_V(\pi^{-1}U)$ is to say that there exists a section $s \in \mathscr{L}(U)$ (which we identify with the section $s_1 \in \mathscr{L}_V(U_1)$) such that the family of functions $\{f_g\}_g$ is computing the section s with respect to the family $\{\varphi_g\}_g$ of trivialisations of $p^{-1}U$. More concretely, if we define a function $f : \pi^{-1}U \to \mathbb{C}$ by $f|_{U_g} = f_g$ then in terms of the commuting triangles of trivialisations we have

$$(gz, f(gz)) = s_g(gz) = T_g(s_1(z)) = T_g(z, f(z)) = (gz, j_g(z)f(z).)$$

Thus a holomorphic section of $p : \mathscr{L} \to X$ is the same thing as a holomorphic function $f : \pi^{-1}U \to \mathbb{C}$ with functional equations

$$f(gz) = j_g(z)f(z), \qquad \text{for all } z \in \pi^{-1}U \text{ and all } g \in G.$$

Let us study the functions j_g more closely. The first thing to notice is that this family of functions satisfies certain identities: the transition functions $\{T_g\}_g$ were defined in such a way that every diagram of the form

[17] If the reader is at all troubled by the author's (ab)use of the term "trivialisation" to refer to a map $\pi^{-1}U \to U_g \times \mathbb{C}$ with U_g (merely!) canonically isomorphic – but not strictly *equal* – to U , they may prefer to think of $\{U_g\}_{g\in G}$ as a family of "charts" for U in which case the φ_g are trivialisations in local coordinates. If they are now doubly-troubled by the author's (ab)use of the term "chart" in the preceding sentence then they are advised to lighten up.

$$\begin{tikzcd}
U_h \times \mathbb{C} \arrow[r, "T_{g_2}"] \arrow[rr, bend left, "T_{g_1 g_2}"] & U_{g_2 h} \times \mathbb{C} \arrow[r, "T_{g_1}"] & U_{g_1 g_2 h} \times \mathbb{C} \\
& p^{-1}U \arrow[ul, "\varphi_h"] \arrow[u, "\varphi_{g_2 h}"'] \arrow[ur, "\varphi_{g_1 g_2 h}"'] &
\end{tikzcd}$$

would commute. Thus

$$(g_1 g_2 x, j_{g_1 g_2}(x) w) = T_{g_1 g_2}(x, w) = T_{g_1} T_{g_2}(x, w) = (g_1 g_2 x, j_{g_1}(g_2 x) j_{g_2}(x) w).$$

To summarise: these functions are related by identities $j_{g_1 g_2}(x) = j_{g_1}(g_2 x) j_{g_2}(x)$ for all $g_1, g_2 \in G$ and for all $x \in \pi^* p^{-1} U$. These identities are collectively known as a **cocycle condition**. Here's why:

Lemma 2.1. *The assignment $g \mapsto j_g$ is a 1-cocycle in group cohomology for G acting on the multiplicative group of nowhere vanishing holomorphic functions on $p^{-1}U$.*[18]

Proof. This is immediate from the basic definitions of group cohomology. These can be found in appendix C.

□

The second thing to notice about the functions j_g is that they give us a complete description of the restricted bundle $p : p^{-1}U \to U$ in terms of a discrete set of data . In order to make this statement precise we describe a general method for generating line bundles on from 1-cocyles.

Let M be a complex manifold and let $\mathcal{O}(M)^\times$ denote the multiplicative group of nowhere vanishing holomorphic functions on M. Let Γ be a group acting freely and properly discontinuously by biholomorphisms on M in such a way that the quotient $\Gamma \backslash M$ is (canonically) a complex manifold.[19] Let $\omega \in H^1(\Gamma, \mathcal{O}(M)^\times)$ be a 1-cocyle and define an action of Γ on $M \times \mathbb{C}$ by the formula

$$\gamma(m, z) := (\gamma m, \omega_\gamma(m) z)$$

where $\omega_\gamma := \omega(\gamma)$.

Proposition 2.5.

$$\begin{array}{rcl} \pi_\omega : \Gamma \backslash \big(M \times \mathbb{C}\big) & \to & \Gamma \backslash M, \\ [m, z] & \mapsto & [m] \end{array}$$

is a holomorphic line bundle on $\Gamma \backslash M$.

Proof. Given our assumptions on the action of Γ on M the map

$$M \times \mathbb{C} \to \Gamma \backslash \big(M \times \mathbb{C}\big), \quad (m, z) \mapsto [m, z]$$

is an isomorphism in a neighbourhood of any point. The corresponding local inverses give local trivialisations of π_ω and are manifestly linear on its fibres.

[18] The G-module structure on the latter group is given by $g(f) := f \circ g^{-1}$.

[19] As before, one may significantly weaken the assumptions on the action if one is prepared to work with orbifolds.

□

We shall refer to such a bundle as the **automorphic line bundle** on $\Gamma\backslash M$ with **factor of automorphy** ω. Returning to the case of V and $X = G\backslash V$, it is a simple matter of unwinding the definitions to verify that the restriction of $p : \mathscr{L} \to X$ to $p^{-1}U$ is isomorphic to the automorphic line bundle on U with factor of automorphy j. Indeed, it follows from our earlier discussions that every line bundle on X is *locally* isomorphic to an automorphic line bundle.

Theorem 6. *The set of isomorphism classes of automorphic line bundles on* $\Gamma\backslash M$ *is in bijection with the first group cohomology* $H^1(\Gamma, \mathcal{O}(M)^\times)$.

Proof. We have already shown that every 1-cocycle determines a line bundle, and so we are tasked with showing that a given pair of automorphic line bundles on $\Gamma\backslash M$ are isomorphic precisely when the ratio of their factors of automorphy is a 1-coboundary.

From the definition of group cohomology a **1-coboundary** is of the form $d^0 f_\gamma(x) = \frac{f(\gamma x)}{f(x)}$ for some $f \in \mathcal{O}(M)^\times$.

Let $\omega : \Gamma \to \mathcal{O}(M)^*, \gamma \mapsto j_\gamma$ be a 1-cocycle, let $f \in \mathcal{O}(X)^\times$ and define a new cocycle ω^f by the formula $\omega^f_\gamma(x) = \omega_\gamma(x)\frac{f(\gamma x)}{f(x)}$. Let $\mathscr{L}_\omega$ and $\mathscr{L}_{\omega^f}$ denote the corresponding line bundles on $\Gamma\backslash M$ and define a function $\varphi : \mathscr{L}_\omega \to \mathscr{L}_{\omega^f}$ by the formula

$$\varphi([x, z]) = [x, f(x)z].$$

This is well defined since

$$\varphi([\gamma x, \omega_\gamma(x)z]) = \varphi([\gamma x, \omega^f_\gamma(x)\frac{f(x)}{f(\gamma x)}z]) = [\gamma x, \omega^f_\gamma(x)f(x)z] = [x, f(x)z] = \varphi([x, z]).$$

Then φ is bijective, holomorphic and linear on the fibres of $\mathscr{L}_\omega$ with holomorphic inverse $[x, z] \mapsto [x, \frac{1}{f(x)}z]$, ie. it is an isomorphism of line bundles on $\Gamma\backslash M$.

Conversely, suppose ω, τ are 1-cocycles and that we are given an isomorphism $\mathscr{L}_\omega \to \mathscr{L}_\tau$ of the form $[x, z] \mapsto [x, \phi(x)z]$. Then ϕ must be nonvanishing (since otherwise it could not restrict to a linear isomorphism on every fibre of $\mathscr{L}_\omega$) and must satisfy $\frac{\phi(\gamma x)}{\phi(x)} = \frac{\tau_\gamma(x)}{\omega_\gamma(x)}$ for all $\gamma \in \Gamma$ (since otherwise it could not be well defined).

□

Remark: The bijection of the theorem can be promoted to a group isomorphism since **(i)** a fibrewise tensor product $\mathscr{L}_{\omega_1} \otimes \mathscr{L}_{\omega_2} \to \Gamma\backslash M$ of automorphic line bundles is once again automorphic with factor of automorphy $\omega_1\omega_2$ and **(ii)** constant 1-cocycles give rise to trivial line bundles.

2.4 Polarizations of complex tori

In this section Λ is a fixed lattice in $\mathbb{C}^g$ and $X = \mathbb{C}^g/\Lambda$ is the corresponding complex torus.

Definition 2.14. *A* **Riemann form** *for the pair* $(\mathbb{C}^g, \Lambda)$ *is a Hermitian form*

$$\begin{array}{rcl} H : \mathbb{C}^g \times \mathbb{C}^g & \to & \mathbb{C}, \\ (z, w) & \mapsto & H(z, w) \end{array}$$

such that $H(\lambda_1, \lambda_2) \in \mathbb{Z}$ *for all* $\lambda_1, \lambda_2 \in \Lambda$.

A **polarization** *of the pair* $(\mathbb{C}^g, \Lambda)$ *is a positive definite Riemann form ie. if a form satisfying* $H(z, z) > 0$ *for all* $z \neq 0 \in \mathbb{C}^g$.

Theorem 7. *Every line bundle* $\mathscr{L}$ *on* X *is automorphic. Up to multiplication by a 1-coboundary, the factor of automorphy of* L *has a factor of automorphy* $\lambda \mapsto j_\lambda$ *for* $\mathscr{L}$ *is of the form*

$$j_\lambda(z) = e^{2\pi i(L(z,\lambda)+J(\lambda))}$$

where $L : \mathbb{C}^g \times \Lambda \to \mathbb{C}$ *and* $J : \Lambda \to \mathbb{C}$ *are such that*

(a) $z \to L(z, \lambda)$ *is* $\mathbb{C}$*-linear for each* $\lambda \in \Lambda$*;*

(b) $\lambda \to L(z, \lambda)$ *is* $\mathbb{Z}$*-linear for all* $z \in \mathbb{C}^g$*;*

(c) $L(\lambda_1, \lambda_2) \equiv L(\lambda_2, \lambda_1) \mod \mathbb{Z}$ *for all* $\lambda_1, \lambda_2 \in \Lambda$*;*

(d) $J(\lambda_1 + \lambda_2) - J(\lambda_1) - J(\lambda_2) \equiv L(\lambda_1, \lambda_2) \mod \mathbb{Z}$ *for all* $\lambda_1, \lambda_2 \in \Lambda$.

Proof. See [Rosen, page 87, theorem B].

□

Condition (b) allows us to extend L to an $\mathbb{R}$-bilinear form on $\mathbb{C}^g$. If $\lambda_1, \ldots, \lambda_{2g}$ is a free generating set for Λ then it is also a basis for $\mathbb{C}^g$ as a $2g$-dimensional real vector space, in which case every $v \in \mathbb{C}^g$ can be written uniquely in the form

$$v = a_1\lambda_1 + \ldots + a_{2g}\lambda_{2g}, \quad a_i \in \mathbb{R}$$

and we define

$$L(z, v) := \sum_{i=1}^{2g} a_i L(z, \lambda_i).$$

Define a function $E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ by the formula $E(z, w) := L(z, w) - L(w, z)$.

Lemma 2.2. *1.* E *is a skew-symmetric* $\mathbb{R}$*-bilinear form on* $\mathbb{C}^g \times \mathbb{C}^g$.

2. E *restricts to a* $\mathbb{Z}$*-bilinear form* $E : \Lambda \times \Lambda \to \mathbb{Z}$.

3. $E : \mathbb{C}^g \times \mathbb{C}^g$ *takes values in* $\mathbb{R}$.

4. $E(iz, iw) = E(z, w)$ *for all* $z, w \in \mathbb{C}^g$.

Proof. (1) Skew symmetry is obvious and we have just now shown that L is $\mathbb{R}$-bilinear.
(2) follows immediately from condition (b) on L.
(3) follows from (1) and (2) since Λ contains a $\mathbb{R}$-basis for $\mathbb{C}^g$.
As for (4), since L is $\mathbb{C}$-linear in the first variable we have

$$E(iz, iw) = i\big[L(z, iw) - L(w, iz)\big]$$

and

$$E(z,w) = -i^2\big[L(z,w) - L(w,z)\big] = i\big[L(iw,z) - L(iz,w)\big].$$

Thus

$$E(iz,iw)-E(z,w) = i\big[L(z,iw)-L(w,iz)+L(iz,w)-L(iw,z)\big] = i\big[E(iz,w)-E(iw,z)\big].$$

But according to (3) both $E(iz,iw) - E(z,w)$ and $E(iz,w) - E(iw,z)$ are real numbers, so $E(iz,iw) - E(w,z) \in \mathbb{R} \cap i\mathbb{R} = \{0\}$.

□

Using these facts it is easy to see that the function $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}^g$ defined by

$$H(z,w) = E(iz,w) + iE(z,w)$$

is a Hermitian form on $\mathbb{C}^g \times \mathbb{C}^g$ taking integer values on $\Lambda \times \Lambda$ ie. it is a Riemann form for the pair $(\mathbb{C}^g, \Lambda)$.

Definition 2.15. *Let $\mathscr{L}$ be a line bundle on $\mathbb{C}^g/\Lambda$ and let L, E and H be as above. We say that H is the* **Riemann form** *associated to $\mathscr{L}$.*

We say that $\mathscr{L}$ is a **polarizing line bundle** *on the complex torus $\mathbb{C}^g/\Lambda$ if the Riemann form associated to $\mathscr{L}$ is a polarization of the pair $(\mathbb{C}^g, \Lambda)$.*

It is a lemma of Frobenius (see [Igusa, §4, page 72]) that if $\mathscr{L}$ is a polarization of $\mathbb{C}^g/\Lambda$ then Λ admits a $\mathbb{Z}$-basis $\lambda_1, \dots, \lambda_{2g}$ with respect to which the corresponding skew-symmetric $\mathbb{R}$-bilinear form $E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ is given by a matrix of the form

$$\begin{pmatrix} & & & & e_1 & & & \\ & & & & & e_2 & & \\ & & & & & & \ddots & \\ & & & & & & & e_g \\ -e_1 & & & & & & & \\ & -e_2 & & & & & & \\ & & \ddots & & & & & \\ & & & -e_g & & & & \end{pmatrix}$$

where each e_i is a strictly positive integer and where $e_1 \mid e_2 \mid \dots \mid e_g$. We shall call such a basis a **symplectic $\mathbb{Z}$-basis** with respect to the polarization. Frobenius' lemma goes on to say that the sequence of integers $(e_1, \dots, e_g)$ does not depend on a choice of symplectic basis, ie. these integers are canonical [Igusa, ibid.].

Definition 2.16. *The* **type** *of a polarization H of $\mathbb{C}^g/\Lambda$ is the sequence of integers $(e_1, e_2, \dots, e_g)$ associated to any symplectic basis with respect to $\mathscr{L}$. A* **principal polarization** *is a polarization of type $(1, 1, \dots, 1)$, ie. a polarization such that the skew symmetric form E is given by the matrix*

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

Definition 2.17. *Let K be a field and let V be either* **(i)** *an algebraic variety over K or else* **(ii)** *a complex manifold if $K = \mathbb{C}$. A* **very ample line bundle**

on V is a line bundle $p : \mathscr{L} \to V$ for which there exists a set of global sections $s_0, s_1, \ldots, s_n : V \to \mathscr{L}$ such that the function

$$\begin{array}{rcl} V & \to & \mathbb{P}^n_{\overline{K}}, \\ x & \mapsto & [s_0(x) : s_1(x) : \ldots : s_n(x)] \end{array}$$

is an embedding. An **ample line bundle** *on V is a line bundle $\mathscr{L}$for which some positive tensor power $\mathscr{L}^{N\otimes}$ is very ample.*

Theorem 8. *(Lefschetz Embedding Theorem). Let $\mathscr{L}$ be a line bundle on a complex torus $X = \mathbb{C}^g/\Lambda$ and let $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ be the associated Riemann form. If H is a polarization of the pair $(\mathbb{C}^g, \Lambda)$ then $\mathscr{L}^{3\otimes}$ is a very ample line bundle on X.*

Thus a polarizable complex torus X is an abelian variety. Conversely, it can be shown that **(i)** for any projective embedding $\vartheta : \mathbb{C}^g \to \mathbb{P}^n$ of a complex torus the Riemann form associated to the pullback along ϑ of the hyperplane line bundle $\mathcal{O}(1)$ on $\mathbb{P}^n$ is a polarization of $(\mathbb{C}^g, \Lambda)$, and **(ii)** every complex abelian variety arises from a polarized complex torus via an embedding of this kind. Henceforth we make no distinction between abelian varieties over $\mathbb{C}$ and polarized complex tori.

Remark: It turns out that *every* 1-dimensional complex torus is an abelian variety (ie. an elliptic curve). Let $\omega_1, \omega_2 \neq 0 \in \mathbb{C}$ be such that $\omega_2/\omega_1 \notin \mathbb{R}$ and consider the complex torus $\mathbb{C}/\Lambda$ where $\Lambda := \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Define a function $E : \mathbb{C} \times \mathbb{C} \to \mathbb{R}$ by

$$E(z, u) = \frac{z \wedge_{\mathbb{R}} u}{\omega_1 \wedge_{\mathbb{R}} \omega_2}.$$

Explicitly, if we write $z = z_1\omega_1 + z_2\omega_2, u = u_1\omega_1 + u_2\omega_2$ for $z_i, u_i \in \mathbb{R}$ then it is trivial to derive the formula

$$E(z, w) = \det \begin{pmatrix} z_1 & u_1 \\ z_2 & u_2 \end{pmatrix}$$

and so E is a skew-symmetric $\mathbb{R}$-bilinear form taking integral values on $\Lambda \times \Lambda$. Thus E is the imaginary part of a positive definite Riemann form $H(z, u) = E(iz, u) + i(E, z, u)$ on $\mathbb{C}$, ie. H is a polarization. It can be shown that any positive definite Riemann form on $\mathbb{C}$ is a multiple of this and so a 1-dimensional complex torus is canonically polarized. This polarization is principal since the imaginary part can be written

$$E(z, u) = \begin{pmatrix} z_1 & z_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}.$$

2.5 Tate modules and ℓ-adic Galois representations

Let A be an abelian variety over a field K and let $\overline{K}$ be a fixed algebraic closure. For each natural number N let $[N] : A(\overline{K}) \to A(\overline{K})$ denote the multiplication by N isogeny and let $A[N]$ be its kernel. In the case that K is a subfield of $\mathbb{C}$, we have $A(\overline{K}) = \mathbb{C}^g/\Lambda$ for some lattice Λ and so $A[N] = \left(\frac{1}{N}\Lambda\right)/\Lambda$. The mental picture this sketches for us in the complex case remains a useful schematic picture for abelian varieties over general fields: if $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ with $p \nmid N$ then $A[N]$ is abstractly isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{2g}$ where g is the dimension of $A \times_K \mathrm{Spec}(\overline{K})$ over $\overline{K}$ [Stevens, §2, examples (2.10)].

Let $\ell \neq \mathrm{char}(K)$ be prime. For each $n \geq 1$ the multiplication by ℓ morphism induces a surjective homomorphism $A[\ell^{n+1}] \xrightarrow{\ell} A[\ell^n]$ and so we have a projective system indexed by $\mathbb{N}$ ending with

$$\ldots \xrightarrow{\ell} A[\ell^3] \xrightarrow{\ell} A[\ell^2] \xrightarrow{\ell} A[\ell] \xrightarrow{\ell} \mathcal{O}.$$

Definition 2.18. *The ℓ-adic* **Tate module** *of A is the projective limit*

$$T_\ell(A) := \varprojlim_n A[\ell^n].$$

Upon fixing compatible isomorphisms $A[\ell^n] \xrightarrow{\sim} \mathbb{Z}/\ell^n\mathbb{Z}$ for all n we obtain an isomorphism $T_\ell(A) \xrightarrow{\sim} (\mathbb{Z}_\ell)^{2g}$.

There is a natural action of the absolute Galois group G_K on $A(\overline{K})$. Recall that a $\overline{K}$-point of A is really a morphism $f : \mathrm{Spec}(\overline{K}) \to A$. By functoriality, the action of G_K on $\overline{K}$ by K-algebra automorphisms induces a action on $\mathrm{Spec}(\overline{K})$ by isomorphisms of K-schemes, whence the canonical action

$$\begin{array}{rcl} G_K \times A(\overline{K}) & \to & A(\overline{K}), \\ (\sigma, f) & \mapsto & f \circ \sigma^{-1}. \end{array}$$

This action descends to an automorphism of $A[\ell^n]$ for all $n \geq 1$: the isogeny $[\ell^n]$ is defined over K and each $\sigma \in G_K$ fixes $A(K)$-pointwise.[20] Each of these actions is continuous for the discrete topology on $A[\ell^n]$ and commutes with the maps $[\ell] : A[\ell^n] \to A[\ell^{n-1}]$ for all $n \geq 1$. By the universal property of projective limits we get a well defined continuous action of G_K on $T_\ell(A)$ for all $l \neq \mathrm{char}(K)$ and by picking bases for each $T_\ell(A)$ as a $\mathbb{Z}_\ell$-module we obtain a system of ℓ-adic Galois representations

$$\rho_{A,\ell} : G_K \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell), \quad \ell \neq \mathrm{char}(K).$$

By tensoring each $T_\ell(A)$ with $\mathbb{Q}$ (note: $\mathbb{Q}_\ell \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$) we obtain corresponding representations of G_K on $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$.

Reduction of abelian varieties.

For any abelian variety A over a number field K there exists a smooth group scheme $\mathrm{Nér}(A)$ over $\mathcal{O}_K$ called the **Néron minimal model** or simply the **Néron model**[21] of A which enjoys the following two properties:

1. The base change $\mathrm{Nér}(A) \times_{\mathcal{O}_K} \mathrm{Spec}(K)$ of $\mathcal{A}$ to K is canonically isomorphic to A.

[20] To say that a point $x \in A(\overline{K})$ belongs to $A[\ell^n]$ is to say that for every choice of local coordinates $x = (x_1, \ldots, x_g)$ the x_i satisfy some set of explicit rational functions with coefficients in K. In these same local coordinates, $\sigma \in G_K$ acts as $(x_1, \ldots, x_g) \mapsto (\sigma x_1, \ldots, \sigma x_g)$ and it follows that G_K acts by permutations on the set of solutions to those rational functions.

[21] We will omit a full definition, but suffice to say that the Néron model satisfies a universal mapping property in the category of group schemes over $\mathcal{O}_K$ and is thus unique up to unique isomorphism by the standard argument. See [Artin] for details.

2. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ the base change Nér$(A) \times_{\mathcal{O}_K}$ Spec$(k_{\mathfrak{P}})$ of $\mathcal{A}$ to the residue field $k_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is a commutative algebraic group over k_p. We emphasise that a commutative algebraic group need not be an abelian variety: the base change of a Nér(A) to k_p may well be neither connected nor projective.

Definition 2.19. *The* **reduction** $\mod \mathfrak{p}$ *of an abelian variety A over K is*

$$A_{\mathfrak{p}} := N\acute{e}r(A) \times_{\mathcal{O}_K} Spec(k_p).$$

By Chevalley's theorem 3, there exists a canonical short exact sequence

$$1 \to N_A \to (A_{\mathfrak{p}})^0 \to A^{ab} \to 1$$

where **(i)** $(A_{\mathfrak{p}})^0$ is the connected component of the identity in A_p, **(ii)** A^{ab} an abelian variety over $k_{\mathfrak{p}}$ and **(iii)** N_A is an affine algebraic normal subgroup of $(A_{\mathfrak{p}})^0$ over $k_{\mathfrak{p}}$.

Definition 2.20. *With the above notation, A is said to have* **good reduction** *at $\mathfrak{p}$ if $N_A = 1$, ie. if the connected component of $A_{\mathfrak{p}}$ is an abelian variety over $k_{\mathfrak{p}}$. Otherwise, A is said to have* **bad reduction** *at $\mathfrak{p}$.*

Example 2.2.

In the case of an elliptic curve E over $\mathbb{Q}$, Chevalley's theorem implies that

$$1 = \dim_{\mathbb{F}_p} E_p = \dim_{\mathbb{F}_p} (E_p)^0 = \dim_{\mathbb{F}_p} N_E + \dim_{\mathbb{F}_p} ab_E.$$

Since there are only two[22] 1-dimensional affine algebraic groups over $\mathbb{F}_p$, it follows that if E has bad reduction at p then either

(a) $E_p \cong \mathbb{G}_m$ and one says that E has **multiplicative bad reduction** at p;

(b) $E_p \cong \mathbb{G}_a$ and one says that E has **additive bad reduction** at p.

Remark: It is known that an abelian variety over $\mathbb{Q}$ has good reduction outside of a finite set of primes. Given the above classification of bad reduction, this allows us to define a useful invariant of an elliptic curve know as its **conductor**.

Definition 2.21. *The* **conductor** *of an elliptic curve E over $\mathbb{Q}$ is the positive integer*

$$N_E := \prod_p p^{R(p)}$$

where p runs over the primes of $\mathbb{Q}$ and the integers $R(p)$ are defined by

$$R(p) = \begin{cases} 0, & \textit{if } E \textit{ has good reduction at } p; \\ 1, & \textit{if } E \textit{ has multiplicative bad reduction at } p; \\ 2, & \textit{if } E \textit{ has additive bad reduction at } p. \end{cases}$$

Remark: There is an obvious alternative method for deriving an algebraic curve over $\mathbb{F}_p$ from an elliptic curve over $\mathbb{Q}$: choose a Weierstraß equation for E over $\mathbb{Z}$ and consider the solution set in $\mathbb{P}^2(\mathbb{F}_p)$ of the reduction $\mod p$ of that equation. It turns out that this simple minded construction agrees with the preceding one: p is a prime of bad reduction for E if and only if the discriminant of any Weierstraß equation for E vanishes $\mod p$, and for all primes of good reduction the reduced equation is a Weierstraß equation for the reduction E_p.

[22] This statement is not technically true since it is possible that E_p is isomorphic to $\mathbb{G}_m$ over an extension of $\mathbb{F}_p$ but not over $\mathbb{F}_p$ itself. The statement becomes true after base change to an algebraic closure $\overline{\mathbb{F}_p}$, and in any case this subtlety will not be of any significance for us.

ℓ-adic cohomology and the L-function of an abelian variety.

Let X be an smooth projective variety over $\mathbb{Q}$. For each prime ℓ and each $j \geq 0$ the natural action of $G_{\mathbb{Q}}$ on $X(\mathbb{Q})$ induces a Galois representation

$$\rho_{A,\ell,j} : G_{\mathbb{Q}} \to \mathrm{GL}\Big(H^j_{\text{ét}}(X, \mathbb{Q}_\ell))\Big).$$

It is a theorem in Grothendieck's Étale / ℓ-adic cohomology that the characteristic polynomial

$$\det(1 - \rho_{X,\ell,j}(\mathrm{Frob}_p)T \mid H^j_{\text{ét}}(X, \mathbb{Q}_\ell)^{I_p}\big) \in \mathbb{Q}_\ell[T]$$

of a Frobenius element at p acting on the maximal unramified-at-p subrepresentation of $H^j_{\text{ét}}(X, \mathbb{Q}_\ell)$ is independent of ℓ so long as $\ell \neq p$ and belongs in each case to $\mathbb{Q}[T]$. When $X = A$ is an abelian variety it is further known [Serre-Tate] that $\rho_{A,\ell,j}$ is unramified at all primes of good reduction for A.

Definition 2.22. *Let X be a projective algebraic variety of dimension g over $\mathbb{Q}$ and let $0 \leq j \leq 2g$. The* **Hasse-Weil L-functions** *of X are the functions $\{L\big(H^j_(X), s\big) \mid 0 \leq j \leq 2g\}$ of a complex variable s defined (for Re(s) sufficiently large) by the infinite product*

$$L\big(H^j(X), s\big) = \prod_p L_p\big(H^j(X), p^{-s}\big)$$

where

$$L_p\big(H^j(X), T\big) := \det\big(1 - T\rho_{X,\ell,j}(Frob_p) \mid H^j_{ét}(X, \mathbb{Q}_\ell)^{I_p}\big)^{-1}$$

for any prime $\ell \neq p$.

Conjecture 2.1. (Hasse-Weil Conjecture) *If X is smooth projective variety over a number field then for every j with $0 \leq j \leq 2\dim X$ there exists a meromorphic function $L_\infty\big(H^j(X), s\big)$ and a positive integer N such that the* **completed L-function**

$$\Lambda\big(H^j(X), s\big) := N^{s/2} L_\infty\big(H^j(X), s\big) L\big(H^j(X), s\big)$$

has a meromorphic continuation to $\mathbb{C}$ which is analytic on $\mathbb{C}\backslash\{1+j/2\}$ and satisfies a functional equation

$$\Lambda\big(H^j(X), s\big) = \pm\Lambda\big(H^j(X), 1 + j - s\big).$$

The following theorem is an analogue of Lefschetz's fixed point formula[23] in the context of ℓ-adic cohomology.

Theorem 9. (**ℓ-adic Lefschetz theorem.**) *Let X be a smooth projective variety over $\mathbb{Q}$ of dimension g and let p be a prime. Then for all primes $\ell \neq p$ and all natural numbers $n \geq 1$ we have the following identity:*

$$\#X(\mathbb{F}_{p^n}) = \#\{x \in X(\overline{\mathbb{Q}}) \mid Frob_p^n(x) = x\} = \sum_{j=0}^{2g} (-1)^j \, Tr\big(Frob_p^n \mid H^j_{ét}(X, \mathbb{Q}_\ell)^{I_p}\big).$$

[23] The original Lefschetz formula (1926) computes the number of fixed points of a continuous endomorphism f of a compact topological space X in terms of the traces of the induced linear endomorphisms of rational homology spaces $H_*^{\text{sing}}(X, \mathbb{Z}) \otimes \mathbb{Q}$.

The ℓ-adic cohomology of an abelian variety is much simpler than that of a general smooth projective variety:

Theorem 10. *Let A be an abelian variety of dimension g over $\mathbb{Q}$. For every prime ℓ we have isomorphisms of $\mathbb{Q}_\ell[G_\mathbb{Q}]$-modules*

(a)

$$H^j_{\acute{e}t}(A, \mathbb{Q}_\ell) \cong H^1_{\acute{e}t}(A, \mathbb{Q}_\ell)^{\wedge_j}, \ \forall 0 \leq j \leq 2g;$$

(b)

$$H^1_{\acute{e}t}(A, \mathbb{Q}_\ell) \cong Hom_{\mathbb{Q}_\ell}\big(T_\ell(A) \otimes \mathbb{Q}, \mathbb{Q}_\ell\big)$$

Proof. See [Milne, §15, theorem 15.1].

□

It follows that all the information that can in principle be extracted from Galois representations on the ℓ-adic cohomologies of an abelian variety is contained in the representations on its first cohomology or, equivalently, on its Tate modules. We are thus motivated to define *the* L-function $L(A, s)$ of A in the following way:

Definition 2.23. *The* **L-function** *of an abelian variety A over $\mathbb{Q}$ is the function of a complex variable s defined (in a maximal right half plane $Re(s) > x_0$) by the infinite product*

$$L(A, s) = \prod_p L_p(A, p^{-s})$$

where

$$L_p(A, T) = \det\big(1 - TFrob_p|V_\ell^{I_p}\big)^{-1}$$

and where V_ℓ can be taken to be either $H^1_{\acute{e}t}(A, \mathbb{Q}_\ell)$ or $T_\ell(A) \otimes \mathbb{Q}$ (with their natural Galois module structures) for any prime $\ell \neq p$.

The following special case of the Hasse-Weil conjecture is known to be true in light of the (elliptic) modularity theorem of Taylor-Wiles and Taylor-Conrad-Breuil-Diamond:

Theorem 11. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Then*

$$\Lambda(E, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$$

has an analytic continuation to an entire function of $\mathbb{C}$ and satisfies the functional equation $\Lambda(E, s) = \pm\Lambda(E, 2 - s)$.

3 Modular Forms

3.1 Symplectic Spaces and Symplectic Groups

Definition 3.1. *A* **symplectic space** *over a field K is a pair (V, h) where V is finite dimensional vector space V over K and where $h : V \times V \to K$ is a non-degenerate, K-bilinear, skew-symmetric form on V. The* **symplectic group** *$Sp(V, h)$ is the group of K-linear automorphisms of V which preserve the form h, ie.*

$$Sp(V, h) = \{g \in GL(V) \mid h(gu, gv) = h(u, v) \textit{ for all } u, v \in V.\}$$

Remark: The dimension of a symplectic space is necessarily even.

If $\mathrm{char}(K) = 0$ then it is always possible to find a basis $\mathcal{B}$ for V such that

$$[h(u, v)]_{\mathcal{B}} = [u]^t_{\mathcal{B}} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} [v]_{\mathcal{B}}$$

where $\dim(V) = 2n$ and where I_n is the $n \times n$ identity matrix [Igusa, §4, lemma 5, pages 71-72]. Such a basis is called a **symplectic basis** for (V, h).

As in §2, a free abelian group Λ in a finite dimensional vector space V over $\mathbb{R}$ or $\mathbb{C}$ is called a **lattice** if some (and hence every) $\mathbb{Z}$-basis for Λ is also an $\mathbb{R}$-basis for V ie. if the natural $\mathbb{R}$-linear map $\mathbb{R} \otimes \Lambda \to V$ is an isomorphism.

Proposition 3.1. *Let (V, h) be a symplectic space over $\mathbb{R}$ with $\dim(V) = 2n$. Suppose that there exists a lattice Λ in V on which h restricts to an integral form $h : \Lambda \times \Lambda \to \mathbb{Z}$. Then there exists a basis $\mathcal{B}$ for Λ with respect to which h is given by a matrix*

$$\begin{pmatrix} 0 & \mathscr{E} \\ -\mathscr{E} & 0 \end{pmatrix}$$

where $\mathscr{E} = diag(e_1, \ldots, e_n)$ is a diagonal matrix with the property that

1. *each e_i is a strictly positive integer;*

2. *$e_1 \mid e_2 \mid \ldots \mid e_g$.*

Moreover, the diagonal matrix $\mathscr{E}$ is uniquely determined by the pair (Λ, h): if $\mathcal{B}'$ is any other such basis for Λ with corresponding diagonal matrix $\mathscr{E}' = diag(e'_1, \ldots, e'_n)$ then $e'_i = e_i$ for all i.

Proof. See [Igusa, Ibid.].

□

In the situation of the proposition, we will say that Λ is an **integral structure** on (V, h).

The upshot is that the category of all symplectic spaces over $\mathbb{R}$ with integral structure breaks up discretely into a countable set of isomorphisms classes. This is analogous to the way in which the category of all finite dimensional vector spaces over a field K breaks up into isomorphism classes parametrised by a single discrete invariant $\dim_K$. This latter phenomenon motivates the definition and study of the general linear groups $\mathrm{GL}_n(K)$, and by pushing this analogy to its logical conclusion we come to the following definition.

Definition 3.2. *Let $g > 0$ be an integer. Let $\mathscr{E}$ and $J_{\mathscr{E}}$ be as above and let $h_{\mathscr{E}}$ denote the corresponding symplectic form on $\mathbb{Z}^{2g}$. The* **general symplectic group** *of* **type** *$\mathscr{E}$ is the group scheme $GSp(\mathscr{E}, \cdot)$ over $\mathbb{Z}$ whose set of R-points for any commutative ring R is the matrix group*

$$GSp(\mathscr{E}, R) = \{M \in GL_{2g}(R) \mid M^t J_{\mathscr{E}} M = \lambda(M)J + \mathscr{E} \text{ for some } \lambda(M) \in R^\times\}$$

of **symplectic similitudes** *of $(R^{2g}, R \otimes_{\mathbb{Z}} h_{\mathscr{E}})$.*

The function $\lambda : \mathrm{GSp}(\mathscr{E}, R) \to R^\times, M \mapsto \lambda(M)$ is necessarily rather special: if $M, N \in \mathrm{GSp}(\mathscr{E}, R)$ then

$$(MN)^t J_{\mathscr{E}}(MN) = N^t(M^t J_{\mathscr{E}} M)N = \lambda(M)N^t J_{\mathscr{E}} N = \lambda(M)\lambda(N)J_{\mathscr{E}}.$$

ie. λ is a group homomorphism. Even better, λ is a morphism of schemes: for each field R and each matrix $M \in \mathrm{GSp}(\mathscr{E}, R)$ the map $M \mapsto \lambda(M)$ is an explicit polynomial function (with integer coefficients, no less) in the entries of M.[24] We have just proved

Proposition 3.2. *λ is a homomorphism $GSp(\mathscr{E}, \cdot) \to GL_1$ of group schemes over $\mathbb{Z}$.*

□

Definition 3.3. *The* **symplectic group** *of* **type** *$\mathscr{E}$ is the group scheme $Sp(\mathscr{E}, \cdot)$ over $\mathbb{Z}$ which sits in the short exact sequence*

$$1 \to Sp(\mathscr{E}, \cdot) \to GSp(\mathscr{E}, \cdot) \xrightarrow{\lambda} GL_1 \to 1.$$

Thus for any commutative ring R we have

$$Sp(\mathscr{E}, R) = \{M \in GL_{2g}(k) \mid M^t JM = J\}.$$

Remark: When $\mathscr{E} = \mathrm{diag}(1, 1, \ldots, 1) = I_g$ we identify $\mathrm{GSp}(I_g, K)$ with the group of all symplectic similitudes of K^{2g} and $\mathrm{Sp}(I_g, K)$ with $\mathrm{Sp}(K^{2g}, H)$ where $H(u, v) = u^t J_I v$ is the standard symplectic form on K^{2g}. We dignify these special cases with a definition:

Definition 3.4. *The* **general symplectic group** *of* **degree** *$2g$ is*

$$GSp_{2g} := GSp(I_g, \cdot).$$

The **symplectic group** *of* **degree** *$2g$ is*

$$Sp_{2g} := Sp(I_g, \cdot).$$

[24] In particular, λ is **(i)** regular as a function on the variety $\mathrm{GSp}(\mathscr{E}, \cdot) \times_{\mathbb{Z}} \mathrm{Spec}(K)$ for any field K, **(ii)** smooth as a function on the real manifold $\mathrm{GSp}(\mathscr{E}, \mathbb{R})$, and **(iii)** holomorphic as a function on the complex manifold $\mathrm{GSp}(\mathscr{E}, \mathbb{C})$.

It is clear from the definition that $\det(M) = \pm 1$ for all $M \in \mathrm{Sp}_{2g}(R)$. In fact, it turns out that $\mathrm{Sp}_{2g}(R)$ is always a subgroup of $\mathrm{SL}_{2g}(R)$.[25]

Proposition 3.3. *Let (V, h) be a symplectic space over $\mathbb{R}$ of dimension $2g$ with an integral structure Λ and type $\mathscr{E}$. There exists a complex structure J on V with respect to which*

$$H : V \times V \to \mathbb{C}, \quad H(u, v) := h(iu, v) + ih(u, v)$$

is a polarization of the complex(ified) torus V/Λ.

Proof. Recall that a complex structure on V is (by definition) a $\mathbb{R}$-linear automorphism $J : V \xrightarrow{\sim} V$ such that $J^2 = -I$, in which case $iu := Ju$ for all $u \in V$. Let $\mathcal{B}$ be a symplectic $\mathbb{Z}$-basis for Λ, so that

$$h(u, v) := [u]_{\mathcal{B}}^t \begin{pmatrix} 0 & \mathscr{E} \\ -\mathscr{E} & 0 \end{pmatrix} [v]_{\mathcal{B}}.$$

One easily checks that the matrix

$$J_I := \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

belongs to $\mathrm{Sp}_(\mathscr{E}, \mathbb{Z})$ for all $\mathscr{E}$ and that the automorphism $J : V \to V$ whose matrix with respect to the basis $\mathcal{B}$ is J_I satisfies $h(Ju, Jv) = h(u, v)$ and that $H(u, v) := h(Ju, v) + ih(u, v)$ is a positive definite hermitian form on complexified vectors space (V, J) and that H integer valued on $\Lambda \times \Lambda$.

□

Recall (from the discussion following lemma 2.2 in §2) that a polarization $H : V \times V \to \mathbb{C}$ of a complex abelian variety V/Λ is always of the form

$$H(u, v) = E(iu, v) + iE(u, v)$$

where $E : V \times V \to \mathbb{R}$ is a non-degenerate, skew-symmetric and $\mathbb{R}$-bilinear form on V which **(i)** restricts to an alternating integral form $E : \Lambda \times \Lambda \to \mathbb{Z}$ and **(ii)** is compatible with the complex structure on V in the sense that $E(iu, iv) = E(u, v)$.

Definition 3.5. *A polarization H of a complex abelian variety V/Λ is said to be of* **type** *$\mathscr{E} = diag(e_1, \ldots, e_g)$ if $E = im(H)$ is represented by the matrix*

$$J_{\mathscr{E}} = \begin{pmatrix} 0 & \mathscr{E} \\ -\mathscr{E} & 0 \end{pmatrix}$$

with respect to some (and thus every) symplectic $\mathbb{Z}$-basis for Λ.

[25] One way to see this is to appeal to the **Pfaffian**. Without going into details, if K is a field with algebraic closure $\overline{K}$ then Pfaffian is a function $\mathrm{Pf} : \mathrm{M}_{2n}(K) \to \overline{K}$ with the property that $\mathrm{Pf}(A^t BA) = (\det A)\mathrm{Pf}(B)$ and $\mathrm{Pf}(A)^2 = \det(A)$ whenever A is a skew symmetric matrix. For $M \in \mathrm{Sp}_{2g}(K)$, $M^t JM = J$ is skew-symmetric and it follows that

$$\mathrm{Pf}(J) = \mathrm{Pf}(M^t JM) = \det(M)\mathrm{Pf}(J) \neq 0,$$

whence $\det M = 1$.

3.2 Siegel Spaces

Definition 3.6. *Let $g \geq 1$ be an integer. The* **Siegel space** *of* **degree** *g is the set*

$$\mathbb{H}^g = \{Z = X + iY \in M_g(\mathbb{C}) \mid Z^t = Z,\ u^t Y u > 0 \text{ for all } u \neq 0 \in \mathbb{R}^g\}$$

of complex, g by g symmetric matrices with positive definite imaginary part.

Remark: $\mathbb{H}^g$ is endowed with a complex manifold structure by declaring that the set inclusion $\mathbb{H}^g \hookrightarrow \mathrm{M}_g(\mathbb{C}) \cong \mathbb{C}^{g^2}$ is a holomorphic embedding.

Theorem 12. (Iwasawa decomposition)[26]

$$Sp_{2g}(\mathbb{R}) = NAK$$

where

1. *$N = N_{2g}$ is the set of all matrices of the form*

$$\begin{pmatrix} U & M \\ 0 & (U^{-1})^t \end{pmatrix}$$

such that **(i)** *$L \in GL_g(\mathbb{R})$ and $(U - I)$ is strictly upper triangular, and* **(ii)** *$M \in M_g(\mathbb{R})$ is such that $(U^{-1}M)^t = U^{-1}M$;*

2.

$$A = A_{2g} = \left\{ diag(a_1, \ldots, a_g, a_1^{-1}, \ldots, a_g^{-1}) \;\middle|\; a_i > 0 \text{ for all } i = 1, \ldots, g \right\};$$

3.

$$K = K_{2g} = \left\{ \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \mid A, B \in M_g(\mathbb{R}), A + iB \in U(g) \right\}.$$

That is, every element $g \in Sp_{2g}(\mathbb{R})$ has a unique factorisation $g = nak$ where $n \in N, a \in A, k \in K$.

Proof. See [Springer, §5, proposition 5.15].

□

Remark: K is a maximal compact subgroup of $\mathrm{Sp}_{2g}(\mathbb{R})$. Since $\mathrm{Sp}_{2g}(\mathbb{R}) \subseteq \mathrm{SL}_{2g}(\mathbb{R})$ and $\mathrm{SO}(2g)$ is a maximal compact subgroup of $\mathrm{SL}_{2g}(\mathbb{R})$ it suffices to check that

$$K = \mathrm{Sp}_{2g}(\mathbb{R}) \cap \mathrm{SO}(2g).$$

If a matrix $X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ belongs to this intersection then from the identities $XX^t = I$ and $X^t J X = J$ we derive

$$AC^t = -BD^t, \quad \text{and} \quad BD^t = DB^t$$

and so

$$A - D = AC^t - DC^t = -D(B^t + C^t).$$

[26] The standard Iwasawa decomposition is the transpose $(NAK)^t = K^t A^t N^t = KAN^t$ of that shown here.

Since both $\mathrm{Sp}_{2g}(\mathbb{R})$ and $\mathrm{SO}(2g)$ are closed under sending X to $-X$ we also have

$$D - A = -(-D)(-B^t - C^t) = -D(B^t + C^t)$$

and it follows that $D = A$ and $B = -C$. That $A+iB$ is unitary follows immediately and so $K = \mathrm{Sp}_{2g}(\mathbb{R}) \cap \mathrm{SO}(2g)$ is a maximal compact subgroup as claimed.

Definition 3.7. *A* **homogeneous space** *is a manifold M such that $M \cong G/H$ for G a Lie group and H a closed subgroup of G. A homogeneous space $M \cong G/H$ is called a* **symmetric space** *for G if there exists an automorphism $\sigma : G \to G$ such that*

(a) $\sigma^2 = id_G$;

(b) H is a union of connected components of the set

$$G^\sigma := \{g \in G \mid \sigma(g) = g\}$$

of σ-fixed points of G.

Examples 3.1.

1. A complex torus $X = \mathbb{C}^g/\Lambda$ is homogeneous but not symmetric: every lie group automorphism of the additive group $\mathbb{C}^g$ is linear and so cannot fix a full lattice Λ without fixing all of $\mathbb{C}^g$.

2. The circle $\mathbb{S}^1$ is a symmetric space with $G = U(1) = \{e^{2\pi ix} \mid x \in \mathbb{R}/\mathbb{Z}\}$. We may take $H = \{1\}$ to the trivial subgroup and σ to be complex conjugation $e^{2\pi ix} \mapsto e^{-2\pi ix}$.

3. $\mathbb{S}^1$ can also be realised as a homogeneous space for $\mathbb{R}$ with $H = \mathbb{Z}$, but it is *not* a symmetric space for $\mathbb{R}$.

Remark: This last example is intended to illustrate that one must specify *how* a given manifold M is to be realised as a homogeneous space before one can ask more refined questions about it. It is thus preferable to either fix a realisation $G/H \xrightarrow{\sim} M$ at the outset, or in the absence of a canonical choice of basepoint in M to think of a homogeneous space as a **fibration**

$$H \to G \to M.$$

Proposition 3.4. *$\mathbb{H}^g$ is a symmetric space for $Sp_{2g}(\mathbb{R})$ which is (non-canonically) isomorphic to $Sp_{2g}(\mathbb{R})/K$ where $K := SO(2g) \cap Sp_{2g}(\mathbb{R})$.*

We begin with a lemma.

Lemma 3.1. *A finite dimensional manifold M is a homogeneous space if and only if M admits a smooth transitive action $G \times M \to M$ by a finite dimensional Lie group G.*

Proof. That a homogeneous space $M \cong G/H$ admits a smooth transitive G-action is trivial. Conversely, suppose that G is a Lie group acting smoothly and transitively (ie. with a single orbit) on M. Fix a point $m_0 \in M$, let H be the stabliser subgroup of m_0 in G and define a map $\varphi : G \to M$ by $\varphi(g) = gm_0$. Then φ is surjective [27] and smooth[28] and its fibres are precisely the cosets of H in G. It follows that φ descends to a smooth bijection $\varphi_H : G/H \to M$. That the inverse (in the category of sets) φ_H is smooth can be seen argued as follows.

- Since M is a manifold every point $x \in M$ has a contractible neighbourhood U.
- Since
$$H \to G \to M$$
is a smooth fibration, any smooth map $Y \xrightarrow{f} M$ with Y contractible factors though a lift $Y \xrightarrow{\hat{f}} G$.
- Applying this to the inclusion $f_U : U \hookrightarrow M$ we get a smooth lift $U \xrightarrow{\hat{f}_U} G$.
- When restricted to U, the function inverse to φ_H is identically equal to the composition $U \xrightarrow{\hat{f}_U} G \xrightarrow{\pi} G/H$ where π is canonical quotient map.
- Since both $\hat{f}_U$ and π are smooth (the latter canonically so) we conclude that the function inverse to φ_H is everywhere locally smooth on M and thus globally smooth (since smooth functions glue).

□ (Lemma)

Proof. (proposition 3.4) The basic strategy should be clear from the lemma: we will construct a smooth transitive action of $\mathrm{Sp}_{2g}(\mathbb{R})$ on $\mathbb{H}^g$ such that K is the stabiliser of a (carefully chosen!) point. If $g \in \mathrm{Sp}_{2g}(\mathbb{R})$ then it follows from the Iwasawa decomposition that g has a unique factorisation

$$g = \begin{pmatrix} I & X \\ 0 & I \end{pmatrix} \begin{pmatrix} V & 0 \\ 0 & (V^t)^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ -B & A \end{pmatrix}$$

where

(a) $X \in \mathrm{M}_g(\mathbb{R})$ is symmetric;

(b) V is an upper triangular matrix with strictly positive diagonal entries;

(c) $\begin{pmatrix} A & B \\ -B & A \end{pmatrix} \in K$.

Indeed, $X = U^{-1}M$ and $V = \mathrm{diag}(a_1, \ldots, a_g)$ in the notation of the Iwasawa decomposition.

[27] By the transitivity assumption.

[28] It is the composition of the embedding $G \hookrightarrow G \times M, g \mapsto (g, m_0)$ of G into $G \times M$ at height m_0 and the smooth action $G \times M \to M$.

Define a function

$$\begin{aligned} \Psi : \mathrm{Sp}_{2g}(\mathbb{R}) \times \mathbb{H}^g &\to \mathbb{H}^g, \\ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \times \tau &\mapsto (A\tau + B)(C\tau + D)^{-1} \end{aligned}$$

For a proof that Ψ is well defined (ie. that $C\tau + D$) is invertible and that $\mathrm{Im}(A\tau + B)(C\tau + D)^{-1} > 0$) see [Klingen, chapter I]. Clearly $\Psi(I, \tau) = \tau$ for all $\tau \in \mathbb{H}^g$ and the following computation

$$\begin{aligned} &\big(A(E\tau + F)(G\tau + H)^{-1}) + B\big)\big(C(E\tau + F)(G\tau + H)^{-1} + D\big)^{-1} \\ &= (AE\tau + AF + BG\tau + BH)(G\tau + H)^{-1}\big(C(E\tau + F)(G\tau + H)^{-1} + D\big)^{-1} \\ &= \big((AE + BG)\tau + AF + BH\big)\big((CE + DG)\tau + CF + DH\big)^{-1} \end{aligned}$$

proves that $\Psi(gh, \tau) = \Psi(g, \Psi(h, \tau))$ for all $g, h \in \mathrm{Sp}_{2g}(\mathbb{R})$ and all $\tau \in \mathbb{H}^g$, ie, that Ψ defines a group action. This action is smooth since if z_{ij} is the coordinate function on $\mathbb{H}^g$ corresponding to the ij^{th} matrix entry then each of the functions

$$\mathrm{Sp}_{2g}(\mathbb{R}) \times \mathbb{H}^g \xrightarrow{\Psi} \mathbb{H}^g \hookrightarrow \mathrm{M}_g(\mathbb{C}) \xrightarrow{z_{ij}} \mathbb{C}$$

is an everywhere well defined rational function of τ and the natural coordintes on $\mathrm{Sp}_{2g}(\mathbb{R})$. Henceforth we abandon the notation Ψ and denote the action by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \tau = (A\tau + B)(C\tau + D)^{-1}.$$

Consider the orbit under this action of the point $iI \in \mathbb{H}^g$.

(a) The stabiliser of iI is K: indeed,

$$\begin{pmatrix} a & B \\ C & D \end{pmatrix} iI = (iA + B)(iC + D)^{-1} = iI \iff iA + B = iD - C$$

and any symplectic matrix of the form $\begin{pmatrix} A & B \\ -B & A \end{pmatrix}$ satisfies $A^tB = B^tA$ and $B^tB + A^tA = I$, in which case

$$(A^t - iB^t)(A + iB) = AA^t + BB^t = I,$$

ie. $A + iB$ is a unitary matrix.

(b) By Cholesky's decomposition theorem for real symmetric matrices, for each $\tau = X + iY \in \mathbb{H}^g$ there exists a unique upper triangular matrix U with positive diagonal entries such that $UU^t = Y$. Let $g_{X,U}$ be the symplectic matrix

$$\begin{pmatrix} I & X \\ 0 & I \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & (U^t)^{-1} \end{pmatrix}.$$

Then

$$g_{X,U} iI = \begin{pmatrix} I & X \\ 0 & I \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & (U^t)^{-1} \end{pmatrix} iI = \begin{pmatrix} I & X \\ 0 & I \end{pmatrix} iUU^t = X + iUU^t = X + iY.$$

Thus $\mathrm{Sp}_{2g}(\mathbb{R})$ acts smoothly on $\mathbb{H}^g$ with a single orbit, and the stabiliser of any point is conjugate to K, ie.

$$K \longrightarrow \mathrm{Sp}_{2g}(\mathbb{R}) \xrightarrow{(g \mapsto giI)} \mathbb{H}^g$$

is a fibration.

The inner automorphism $\sigma(g) := JgJ^{-1}$ of $\mathrm{Sp}_{2g}(\mathbb{R})$ has order 2, and the identity

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = J \begin{pmatrix} A & B \\ C & D \end{pmatrix} J^{-1} = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix}$$

holds in $\mathrm{Sp}_{2g}(\mathbb{R})$ if and only if $\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \in K$, whence $K = \mathrm{Sp}_{2g}(\mathbb{R})^\sigma$. We conclude that $\mathbb{H}^g$ is a symmetric space for $\mathrm{Sp}_{2g}(\mathbb{R})$.

□

3.3 Universal Families and Moduli Spaces of Polarized Abelian Varieties

Throughout this section g is a fixed positive integer and $\mathscr{E} = \mathrm{diag}(e_1, \ldots, e_g)$ denotes a fixed polarization type.

Let $(V/\Lambda, H)$ be a complex abelian variety of dimension g with polarization H of type $\mathscr{E}$. For each symplectic $\mathbb{Z}$-basis $\mathcal{B}_\Lambda = \{\lambda_1, \ldots, \lambda_{2g}\}$ for Λ we have (care of [Igusa, §4, pages 72-74]) the following $\mathbb{C}$-basis $\mathcal{B}_V$ for V:

$$\mathcal{B}_V := \{\lambda_{g+i} \mid 1 \leq i \leq g\}.$$

Consider the function Ω from the set of symplectic $\mathbb{Z}$-bases for Λ to the set $\mathrm{M}_{2g \times g}(\mathbb{C})$ of $2g \times g$ complex matrices defined by the rule

$$\mathcal{B}_\Lambda = \{\lambda_1, \ldots, \lambda_{2g}\} \mapsto \Omega(\mathcal{B}_\Lambda) := \begin{pmatrix} [\lambda_1]_{\mathcal{B}} \\ \vdots \\ [\lambda_g]_{\mathcal{B}} \\ [\lambda_{g+1}]_{\mathcal{B}} \\ \vdots \\ [\lambda_{2g}]_{\mathcal{B}} \end{pmatrix}$$

where $[u]_{\mathcal{B}_V} \in \mathbb{C}^g$ denotes the *row* vector of coordinates of $u \in V$ with respect to $\mathcal{B}_V$

Proposition 3.5.

$$\Omega(B_\Lambda) = \begin{pmatrix} \tau_{\mathcal{B}} \\ I \end{pmatrix} \quad \textit{for some } \tau_{\mathcal{B}} \in \mathbb{H}^g.$$

Proof. That rows $g+1$ through $2g$ of $\Omega(\mathcal{B}_\Lambda)$ form a g by g identity matrix is obvious. The claim about the first g rows is proved on pages 72-74 of [Igusa] .

□

If $\mathcal{B}'_\Lambda = \{\lambda'_1, \ldots, \lambda'_{2g}\}$ is some other symplectic $\mathbb{Z}$-basis for Λ then there exists a unique integral change of (symplectic) basis matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(\mathscr{E}, \mathbb{Z})$$

satisfying

$$\begin{pmatrix} [\lambda'_1]_{\mathcal{B}_V} \\ \vdots \\ [\lambda'_g]_{\mathcal{B}_V} \\ [\lambda'_{g+1}]_{\mathcal{B}_V} \\ \vdots \\ [\lambda'_{2g}]_{\mathcal{B}_V} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} \tau_{\mathcal{B}} \end{pmatrix} = \begin{pmatrix} A\tau_{\mathcal{B}} + B \\ C\tau_{\mathcal{B}} + D \end{pmatrix}.$$

From this we obtain the identity

$$\tau_{\mathcal{B}'} = (A\tau_{\mathcal{B}} + B)(C\tau_{\mathcal{B}} + D)^{-1}.$$

We also observe that for all $v \in V$,

$$[v]^t_{\mathcal{B}_V} = [v]^t_{\mathcal{B}'_V} \begin{bmatrix} \lambda'_{g+1} \\ \vdots \\ \lambda'_{2g} \end{bmatrix}_{\mathcal{B}_V} = [v]^t_{\mathcal{B}'_V} \left(C \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_g \end{bmatrix}_{\mathcal{B}_V} + D \begin{bmatrix} \lambda_{g+1} \\ \vdots \\ \lambda_{2g} \end{bmatrix}_{\mathcal{B}_V} \right) = [v]^t_{\mathcal{B}'_V} \big(C\tau_{\mathcal{B}} + D \big).$$

This gives us an explicit change of basis formula, namely

$$[v]_{\mathcal{B}'_{\mathcal{V}}} = [v]_{\mathcal{B}_{\mathcal{V}}} (C\tau_{\mathcal{B}} + D)^{-1}.$$

For each $\tau \in \mathbb{H}^g$ let

$$\Lambda_{\tau,\mathscr{E}} := \mathbb{Z}^g \tau + \mathbb{Z}^g$$

be the lattice generated by the rows $\tau_1, \ldots, \tau_g$ of τ and by $\mathbb{Z}^g \subseteq \mathbb{C}^g$ and endow $\Lambda_{\tau,\mathscr{E}}$ with the fixed ordered $\mathbb{Z}$ basis

$$\mathcal{B}_\tau := \big(\tau_1, \ldots, \tau_g, z_1, \ldots, z_g\big)$$

where $z_j := (\delta_{1j}, \ldots, \delta_{gj})$ with δ_{ij} denoting the Krönecker delta. Let $E_{\tau,\mathscr{E}} : \mathbb{C}^g \to \mathbb{R}$ be the alternating $\mathbb{R}$-bilinear form on $\mathbb{C}^g$ given by

$$E_{\tau,\mathscr{E}}(u, v) := [u]^t_{\mathcal{B}_\tau} \begin{pmatrix} 0 & \mathscr{E} \\ -\mathscr{E} & 0 \end{pmatrix} [v]_{\mathcal{B}_\tau}$$

where $\mathcal{B}_\tau$ is thought of as an $\mathbb{R}$ basis for $\mathbb{C}^g$.

Theorem 13. *The function*

$$H_{\tau,\mathscr{E}} : \mathbb{C}^g \to \mathbb{C}, \quad H_{\tau,\mathscr{E}}(u, v) := E_{\tau,\mathscr{E}}(iu, v) + E_{\tau,\mathscr{E}}(u, v)$$

is a positive definite Riemann form with respect to the pair $\big(\mathbb{C}^g, \Lambda_{\tau,\mathscr{E}}\big)$. Thus the complex torus $A_{\tau,\mathscr{E}} := \mathbb{C}^g/\Lambda_{\tau,\mathscr{E}}$ is an abelian variety over $\mathbb{C}$ with a fixed polarization of type $\mathscr{E}$.

Proof. See [M.Rosen, §6, pages 97-98] and [J.Igusa, §4, pages 72-72].

□

The following lemma is more or less a tautology at this point. We state it for emphasis.

Lemma 3.2. *Let $A := V/\Lambda$ be a g dimensional abelian variety over $\mathbb{C}$ and let $H : V \to \mathbb{C}$ be a polarization of A of type $\mathscr{E}$. Then for each choice of symplectic $\mathbb{Z}$-basis $\mathcal{B}_\Lambda$ the function*

$$\begin{aligned} A &\to A_{\tau_\mathcal{B},\mathscr{E}}, \\ z \mod \Lambda &\mapsto [z]_\mathcal{B} \mod \Lambda_{\tau,\mathscr{E}} \end{aligned}$$

is an isomorphism of $\mathscr{E}$-polarized abelian varieties.

□

Let $\mathcal{A}_{g,\mathscr{E}}$ denote the set of pairs $(\tau, z \mod \Lambda_{\tau,\mathscr{E}})$ where

(a) $\tau \in \mathbb{H}^g$;

(b) $z \in A_{\tau,\mathscr{E}}$.

Thus $\mathcal{A}_{g,\mathscr{E}}$ can be though of as the union of all the $\mathscr{E}$-polarized abelian varieties $A_{\tau,\mathscr{E}}$. Let $\mathrm{Sp}(\mathscr{E},\mathbb{Z})$ act on $\mathcal{A}_{g,\mathscr{E}}$ according to the formula

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} (\tau, z) := \left((A\tau + B)(C\tau + D)^{-1}\ , z(C\tau + D)^{-1}\right).$$

Definition 3.8. *A* **family of abelian varieties** *over a field K is a morphism $\pi : \mathfrak{A} \to \mathfrak{X}$ of K-schemes with a section $\mathcal{O} : \mathfrak{X} \to \mathfrak{A}$ such that for each K-point $x \in \mathfrak{X}$ the fibre $\pi^{-1}(x) := x \times_\mathfrak{X} \mathfrak{A}$ is an abelian variety over K with identity element $\mathcal{O}(x)$. A family $\pi : \mathfrak{A} \to \mathfrak{X}$ of abelian varieties over K is called a* **universal family** *if every abelian variety A over K is isomorphic to exactly one fibre of π.*

Remark: One can also consider universal families for restricted classes of abelian varieties. For instance, if K is a field and $\pi : \mathfrak{A} \to \mathfrak{X}$ is a universal family of abelian varieties over K then there is a subfamily $\pi_g : \mathfrak{A}_g \to \mathfrak{X}_g$ of abelian varieties over K of fixed dimension g. By specifying additional data (eg. polarization type) we obtain yet smaller universal families.

Theorem 14.

$$\begin{aligned} \pi : Sp(\mathscr{E},\mathbb{Z})\backslash\mathcal{A}_{g,\mathscr{E}} &\to Sp(\mathscr{E},\mathbb{Z})\backslash\mathbb{H}^g, \\ [\tau, z] &\mapsto [\tau] \end{aligned}$$

is a universal family of g-dimensional $\mathscr{E}$-polarized abelian varieties over $\mathbb{C}$ with identity section $\mathcal{O}[\tau] \mapsto [\tau, 0]$.

Proof. By proposition 3.5, whenever V/Λ is a g-dimensional $\mathscr{E}$-polarized abelian variety then every choice of symplectic $\mathbb{Z}$-basis $\mathcal{B}$ for Λ determines a point $\tau_\mathcal{B} \in \mathbb{H}^g$ together with an isomorphism

$$V/\Lambda \xrightarrow{\sim} \mathbb{C}^g/\Lambda_{\tau_\mathcal{B},\mathscr{E}} = A_{\tau_\mathcal{B},\mathscr{E}} \cong \pi^{-1}(\tau_\mathcal{B})$$

of $\mathscr{E}$-polarized abelian varieties over $\mathbb{C}$. By construction the set

$$\{\tau_\mathcal{B} \in \mathbb{H}^g \mid \mathcal{B} \text{ is a symplectic } \mathbb{Z}\text{-basis for } V/\Lambda\}$$

is a single orbit in $\mathbb{H}^g$ under the action of $\mathrm{Sp}(\mathscr{E},\mathbb{Z})$ and so the set of all $A_{\tau,\mathscr{E}}$ to which A is isomorphic as a $\mathscr{E}$-polarized abelian variety comprises exactly one fibre of π.

□

One can paraphrase theorem 14 as follows: $\mathrm{Sp}(\mathscr{E},\mathbb{Z})\backslash\mathbb{H}^g$ is a **coarse moduli space** of g-dimensional complex abelian varieties with $\mathscr{E}$-type polarisation. In general one cannot infer that $\mathrm{Sp}(\mathscr{E},\mathbb{Z})\backslash\mathbb{H}^g$ is a **fine moduli space** since there might well exist g-dimensional complex abelian varieties which are *non-uniquely* isomorphic (as $\mathscr{E}$-polarized abelian varieties) to a fibre of $\pi : \mathrm{Sp}(\mathscr{E},\mathbb{Z})\backslash\mathcal{A}_{g,\mathscr{E}} \to \mathrm{Sp}(\mathscr{E},\mathbb{Z})\backslash\mathbb{H}^g$. This phenomenon is best demonstrated by example.

3.4 Example: Level Structures for Elliptic curves

We have already seen that every elliptic curve over $\mathbb{C}$ carries a principal polarization, so we may think of

$$\pi : \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{A}_1 \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^1$$

(where $\mathcal{A}_1 := \mathcal{A}_{1,I}$) as a universal family for all elliptic curves over $\mathbb{C}$.

The point $\frac{-1+i\sqrt{3}}{2} \in \mathbb{H}^1$ has a non-trivial stabiliser in $\mathrm{SL}_2(\mathbb{Z})$: for instance, we have

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \frac{-1+i\sqrt{3}}{2} = \frac{-2}{i\sqrt{3}+1} = \frac{-2(1-i\sqrt{3})}{(1+i\sqrt{3})(1-i\sqrt{3})} = \frac{-2+2i\sqrt{3}}{4} = \frac{-1+i\sqrt{3}}{2}.$$

Since $z \mapsto z\big(\frac{-1+i\sqrt{3}}{2}+1\big)^{-1}$ is not the identity function on $A_{\frac{-1+i\sqrt{3}}{2}}$ it follows that the elliptic curve $A_{\frac{-1+i\sqrt{3}}{2}}$ has non-trivial automorphisms and that no elliptic curve E can ever be *uniquely* isomorphic to $A_{\frac{-1+i\sqrt{3}}{2}}$.

Thus the "coarseness' of the moduli space can be traced to a lack of freeness in the action of $\mathrm{Sp}(\mathscr{E},\mathbb{Z})$ on $\mathbb{H}^g$. A useful trick for fixing this deficiency is to consider not just $\mathscr{E}$-polarised abelian varieties but $\mathscr{E}$-polarised abelian varieties together with a so-called **level structure**. Rather than attempting to give a uniform definition of a "level structure" [29] we shall illustrate how the technique applies to the moduli space of elliptic curves.

Let N be a positive integer and consider the following subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

(a)

$$\begin{aligned} \Gamma(N) &:= \ker\big(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\big) \\ &= \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N\Big\}, \end{aligned}$$

(b)

$$\Gamma_1(N) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N\Big\},$$

(c)

$$\Gamma_0(N) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N\Big\},$$

[29] Level structures tends to be something defined in an *ad hoc* manner for the purposes of refining a specific moduli problem. It is hoped that the examples presented here make the "philosphy" of level structures clear.

where "$*$" denotes an arbirary integer. Notice that $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$ in this notation, and that we have a chain of inclusions

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \Gamma(1).$$

Thus we have a diagram of (generically ramified) coverings

$$\begin{tikzcd}
\Gamma(N)\backslash\mathbb{H}^1 \arrow[r] \arrow[dr] & \Gamma_1(N)\backslash\mathbb{H}^1 \arrow[r] \arrow[d] & \Gamma_0(N)\backslash\mathbb{H}^1 \arrow[dl] \\
 & \Gamma(1)\backslash\mathbb{H}^1 &
\end{tikzcd}$$

Lemma 3.3. *For $N \geq 2$ (resp. $N \geq 3$) the groups $\Gamma(N)$ and $\Gamma_1(N)$ (resp. $\Gamma_0(N)$) act freely on $\mathbb{H}^1$.*

Proof. See [Husemöller, Chapter 11, §2, prop. 2.5].

□

For $\tau \in \mathbb{H}^1$ we make the following definitions.

1. E_τ is the elliptic curve $\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$;
2. $P(\tau) := \frac{\tau}{N}$;
3. $Q(\tau) := \frac{1}{N}$
4. $C(\tau)$ is the order N subgroup of $E(\tau)$ generated by $Q(\tau)$.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{H}^1\mathbb{C} \times \mathbb{C}$ according to the formula

$$\gamma(\tau, u, w) := \Big(\gamma\tau, \frac{u}{c\tau + d}, \frac{w}{c\tau + d}\Big)$$

where the action of γ on $\mathbb{H}^1$ is the usual one eg. $\gamma(\tau) = (a\tau) + b)(c\tau + d)^{-1}$.

Suppose that γ satisfies

$$\gamma(E_\tau, z \bmod \mathbb{Z}\tau{+}\mathbb{Z}, P(\tau), Q(\tau) = \big(E(\gamma\tau), P(\gamma\tau) \bmod \mathbb{Z}\gamma\tau{+}\mathbb{Z}, Q(\gamma\tau) \bmod \mathbb{Z}\gamma\tau{+}\mathbb{Z}\big) \tag{1}$$

Then there exist integers m_1, m_2, m_3, m_4 such that

(a)

$$\frac{1}{N}(c\tau + d)^{-1} = \frac{1}{N} + m_1(a\tau + b)(c\tau + d)^{-1} + m_2;$$

(b)

$$\frac{\tau}{N}(c\tau + d)^{-1} = \big(\frac{1}{N} + m_3\big)(a\tau + b)(c\tau + d)^{-1} + m_4.$$

From (a) we derive $d = 1 - N(m_1 b + m_2 d)$ and $c = -N(m_1 a + m2d)$ and from (b) we derive $a = 1 + N(m_3 c + m_2 a)$ and $b = N(m_3 d + m_4 b)$. In other words we have congruences $a \equiv d \equiv 1 \mod N$ and $c \equiv b \equiv 0 \mod N$. Conversely, one easily checks that equation (1) holds for arbitrary $\gamma \in \Gamma(N)$.

Lemma 3.4. *Let $E = \mathbb{C}/\Lambda$ be an elliptic curve over $\mathbb{C}$ with a fixed "basis" ω_1, ω_2 for its submodule $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ of N-torsion points. Then every choice of $\mathbb{Z}$-basis $\tilde{\omega_1}, \tilde{\omega_2}$ for $\Lambda[N] := \{z \in \mathbb{C} \mid Nz \in \Lambda\}$ satisfying $\tilde{\omega_i} \equiv \omega_i \mod \Lambda$ induces an isomorphism $\psi : E \overset{\sim}{\to} E(\tau)$ $(\tau \in \mathbb{H}^g)$ with $\psi_(\omega_1) = P(\tau) \mod \mathbb{Z}\tau + \mathbb{Z}$ and $\psi(\omega_2\Lambda) = Q(\tau) \mod \mathbb{Z}\tau + \mathbb{Z}$.*

Proof. The only difficult thing about this lemma is unpacking the unfortunate notation. If $\tilde{\omega_1}$ and $\tilde{\omega_2}$ are as in the statement then $\mathcal{B} := \{N\tilde{\omega_1}, N\tilde{\omega_2}\}$ is a $\mathbb{Z}$-basis for $\mathbb{C}/\Lambda$. By proposition 3.5 we associate to $\mathcal{B}$ a unique point $\tau \in \mathbb{H}^1$ and an isomorphism $\psi : E \overset{\sim}{\to} E(\tau_{\mathcal{B}})$. That $\psi(\omega_1) = P(\tau)$ and $\psi_(\omega_2) = Q(\tau)$ is immediate (under the assumption that $\mathcal{B}$ reduces mod Λ to the set $\{\omega_1, \omega_2\}$) from our construction of the isomorphism ψ.

□

Combining lemma 3.4 with the computation of congruences which preceded it we obtain the following.

Theorem 15. *Let*

$$\mathcal{A}_1(\Gamma(N)) := \{(\tau, z, P(\tau), Q(\tau) \mid \tau \in \mathbb{H}^1,\ z \in \mathbb{C} \mod \mathbb{Z}\tau + \mathbb{Z}\} \subseteq \mathcal{A}_1 \times \mathbb{C} \times \mathbb{C}.$$

Then

$$\pi_{\Gamma(N)} : \Gamma(N)\backslash\mathcal{A}_1(\Gamma(N)) \to \Gamma(N)\backslash\mathbb{H}^1$$

is a universal family of triples (E, P, Q) where

1. *E is an elliptic curve over $\mathbb{C}$;*

2. *$P, Q \in E$ are generators for the N-torsion submodule $E[N]$ of E.*

□

Corollary 3.1. *Let $SL_2(\mathbb{Z})$ act on $\mathcal{A}_1 \times \mathbb{C}$ like so:*

$$\gamma(\tau, z \in \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, p) := \big(\gamma\tau, z(c\tau + d)^{-1} \in \mathbb{C}/\mathbb{Z}\gamma\tau + \mathbb{Z}, p(c\tau + d)^{-1}\big).$$

Define

$$\mathcal{A}_1(\Gamma_1(N)) := \{(\tau, z \in \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, P(\tau)\} \subseteq \mathcal{A}_1 \times \mathbb{C}.$$

Then

$$\pi_{\Gamma_1(N)} : \Gamma_1(N)\backslash\mathcal{A}_1(\Gamma_1(N)) \to \Gamma(1)\backslash\mathbb{H}^1$$

is a universal family of pairs (E, P) where

1. *E is an elliptic curve over $\mathbb{C}$;*

2. *P is a point of (exact) order N in E.*

Proof. This all but falls out from theorem 15 upon forgetting the second generator for $E[N]$. Returning to the derivation of congruences preceding lemma 3.4, if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is to satisfy $P(\gamma\tau) = P(\tau)(cz+d)^{-1}$ then we must have $d \equiv 1, c \equiv 0 \mod N$. From this one infers (given that γ must be invertible mod

By forgetting the point P of order N while still keeping track of the cyclic subgroup it generates one obtains

Corollary 3.2. *Let $\mathcal{A}_1(\Gamma_0(N))$ be the set*

$$\mathcal{A}_1(\Gamma_0(N)) := \{(\tau, z, C(\tau)) \mid \tau \in \mathbb{H}^1, z \in E(\tau)\}$$

where $C(\tau)$ is the cyclic subgroup of order N in $E(\tau)$ defined in the discussion preceding 3.4 . Then $\Gamma_0(N)$ acts on $\mathcal{A}_1(\Gamma_0(N))$ according to the definition

$$\gamma(\tau, z, C(\tau)) := \big(\gamma\tau, z(c\tau + d)^{-1}, C(\gamma\tau\big)$$

and the projection

$$\pi_{\Gamma_0(N)} : \Gamma_0(N)\backslash\mathcal{A}_1(\Gamma_0(N)) \to \Gamma_0(N)\backslash\mathbb{H}^1$$

is a universal family of elliptic curves over $\mathbb{C}$ with a choice of cyclic subgroup of order N.

Proof. The proof follows from corollary 3.1 in a fashion more or less identical to the way corollary 3.1 followed from theorem 15. We omit the details.

□

Combining these results with the lemma 3.3 we arrive at the following conclusion.

Theorem 16. *(a) For $N \geq 2$ the space*

$$Y(N) := \Gamma(N)\backslash\mathbb{H}^1$$

is a fine moduli space classifying elliptic curves E over $\mathbb{C}$ with a fixed basis P, Q for their N-torsion submodule $E(N)$.

(b) For $N \geq 2$ the space

$$Y_1(N) := \Gamma_1(N)\backslash\mathbb{H}^1$$

is a fine moduli space classifying elliptic curves E over $\mathbb{C}$ with a chosen point $P \in E$ of exact order N.

(c) For $N \geq 3$ the space

$$Y_0(N) := \Gamma_0(N)\backslash\mathbb{H}^1$$

is a fine moduli space[30] *classifying elliptic curves E over $\mathbb{C}$ with a chosen cyclic subgroup C of order N.*

3.5 Modular Forms

The goal of the present section is to replace the *ad hoc* definition of modular forms from §1 with the following uniform definition: modular forms are holomorphic global sections of a certain natural family of automorphic line bundles [31] on moduli spaces of polarised abelian varieties (with or without level structure).

[30] Technically this is not quite true since every elliptic curve has an automorphism $E \xrightarrow{-1} E, P \mapsto -P$ and this automorphism clearly fixes any cyclic subgroup of E. This is a minor concern which can be solved by passing to a certain double cover of $Y_0(N)$.

[31] We choose to discuss scalar valued modular forms only. It is not difficult to formulate a definition of automorphic vector bundles of rank > 1 and thus adapt our presentation to include vector valued modular forms.

Definition 3.9. *A* **locally symmetric space** *is a space of the form* $\Gamma\backslash G/K$ *where* **(i)** G *is a Lie group,* **(ii)** K *a Lie subgroup of* G *(eg. a maximal compact subgroup) and* **(iii)** Γ *is a discrete subgroup of* G.

This definition encompasses the moduli spaces of *principally polarized* abelian varieties since we have seen how to realise each Siegel space $\mathbb{H}^g$ as a symmetric space $\mathrm{Sp}_{2g}(\mathbb{R})/\big(SO(2g) \cap \mathrm{Sp}_{2g}(\mathbb{R})$. So as to extend this definition over moduli spaces of abelian varieties with arbitrary polarizations we substitute "surrogate" moduli spaces of polarised abelian varieties that can be realised as quotients of $\mathbb{H}^g$ by discrete (but generically non-integral) subgroups of $\mathrm{Sp}_{2g}(\mathbb{Q})$.

Lemma 3.5. *$Sp(\mathscr{E},\mathbb{Z})$ is conjugate in $GL_{2g}(\mathbb{Q})$ to a subgroup of $Sp_{2g}(\mathbb{Q})$.*

The matrix

$$I_{\mathscr{E}} := \begin{pmatrix} I & 0 \\ 0 & \mathscr{E} \end{pmatrix}$$

is an element of $\mathrm{GL}_{2g}(\mathbb{Q})$ and satisfies $I_{\mathscr{E}} J_I I_{\mathscr{E}} = J_{\mathscr{E}}$. If $M \in \mathrm{Sp}(\mathscr{E},\mathbb{Z})$ then we have

$$\begin{aligned} (I_{\mathscr{E}} M I_{\mathscr{E}}^{-1})^t J_I (I_{\mathscr{E}} M I_{\mathscr{E}}^{-1}) &= I_{\mathscr{E}}^{-1} M^t I_{\mathscr{E}}^t J_I I_{\mathscr{E}} M I_{\mathscr{E}}^{-1} \\ &= I_{\mathscr{E}}^{-1} M^t J_{\mathscr{E}} M I_{\mathscr{E}}^{-1} \\ &= I_{\mathscr{E}}^{-1} J_{\mathscr{E}} I_{\mathscr{E}}^{-1} \\ &= J_I. \end{aligned}$$

□

Henceforth we identify the coarse moduli space $\mathrm{Sp}(\mathscr{E},\mathbb{Z})\backslash\mathbb{H}^g$ with $\Gamma(\mathscr{E})\backslash\mathbb{H}^g$ where $\Gamma(\mathscr{E}) := I_{\mathscr{E}}\mathrm{Sp}_{2g}(\mathscr{E},\mathbb{Z})I_{\mathscr{E}}^{-1} \subseteq \mathrm{Sp}_{2g}(\mathbb{Q})$ is as in lemma 3.5. The kind of moduli spaces one obtains in this way are of the form $\Gamma\backslash\mathbb{H}^g$ where Γ is an **arithmetic subgroup** of $\mathrm{Sp}_{2g}(\mathbb{Q})$.

Definition 3.10. *Let G be an group scheme over $\mathbb{Z}$. An* **arithmetic subgroup** *of G is a subgroup Γ of $G(\mathbb{Q})$ such that if we write $\Gamma' := \Gamma \cap G(\mathbb{Z})$ then Γ' has finite index in both $G(\mathbb{Z})$ and Γ, ie.*

$$[G(\mathbb{Z}) : \Gamma'] < \infty \quad \textit{and} \quad [\Gamma : \Gamma'] < \infty.$$

It is precisely spaces of the form $\Gamma\backslash\mathbb{H}^g$ for arithmetic $\Gamma \subseteq \mathrm{Sp}_{2g}(\mathbb{Q})$ on which we shall define our "certain natural family" of automorphic line bundles. We will now attempt to explain what exactly we mean by "natural."

Lemma 3.6. *Let G be a group acting smoothly on a manifold M. For each $g \in G$ and $m \in M$ let $\mathfrak{D}g|_m$ denote the derivative (ie. Jacobian matrix) of the action of g on M at the point m. Then the function*

$$G \times M \to \mathbb{R}, \quad (g,m) \mapsto \det\big(\mathfrak{D}g|_m\big)$$

represents a class in the 1st group cohomology $H^1(G,\mathcal{O}(M))$ of G with coefficients in the ring $\mathcal{O}(M)$ of smooth real valued functions on M.

Proof. If $g,h \in G$ and $m \in M$ then $\det\big(\mathfrak{D}gh|_m\big) = \big(\mathfrak{D}g|_{hm}\mathfrak{D}h|_m\big) = \big(\mathfrak{D}g|_{hm}\big)\big(\mathfrak{D}h|_m\big)$. This is precisely the cocycle condition.[32]

[32] See appendix C.

□

Remark Both the statement and proof of this lemma go through mutatis mutandis for complex manifolds with holomorphic actions.

Our intention is that lemma 3.6 be understood in the following way: whenever M is a a locally symmetric space of the form $\Gamma\backslash G/K$ with Γ discrete then the cocycle $\gamma \mapsto \det\big(\mathfrak{D}\gamma\big)$ is a factor of automorphy for the (eminently natural) line bundle $\det\mathfrak{D}$ which encodes the derivatives of the action of Γ on M.

Proposition 3.6. *Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2g}(\mathbb{R})$ let $\mathfrak{D}M_\tau$ denote the derivative of the action of M on $\mathbb{H}^g$ at the point τ. Then*

$$\det\mathfrak{D}M_{\tau_0} = \det(C\tau_0 + D)^{-g-1}.$$

Proof. See [Klingen, I.3, pages 35-36].

□

Definition 3.11. *The* **standard**[33] **factor of automorphy** *for the action of $Sp_{2g}(\mathbb{R})$ on $\mathbb{H}^g$ is*

$$\begin{aligned} j : Sp_{2g}(\mathbb{Q}) &\rightarrow \mathcal{O}(\mathbb{H}^g)^\times, \\ \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} &\mapsto j_\gamma(\tau) := \det(C\tau + D). \end{aligned}$$

Definition 3.12. *Let $k \in \mathbb{Z}$ and let $\Gamma \subseteq Sp_{2g}(\mathbb{Q})$ be a discrete group. A* **modular form** *of* **weight** *k and level Γ is a holomorphic global section of the automorphic line bundle $\mathscr{L}_{j^k}(\Gamma)$ on $\Gamma\backslash\mathbb{H}^g$ with factor of automorphy j^k.*

The vector space over $\mathbb{C}$ of all modular forms of weight k and level Γ will be denoted $M_k(\Gamma)$.

Remarks:

1. The space of modular forms of weight k and level Γ can be identified with $H^0\big(\Gamma\backslash\mathbb{H}^g, \mathscr{L}_{j^k}(\Gamma)\big)$.[34]

2. If $f \in M_k(\Gamma)$ and $g \in M_j(\Gamma)$ then it is trivial to check that $fg \in M_{k+j}(\Gamma)$. We can thus think each $M_k(\Gamma)$ as a homogeneous summand in a $\mathbb{Z}$-graded $\mathbb{C}$-algebra
$$M_*(\Gamma) := \bigoplus_k M_k(\Gamma).$$

From the preceding geometric definition one derives the following "classical" looking definition:

[33] The term "standard" is entirely our own and thus entirely *non*-standard in the literature. Indeed, no one else seems to have bothered to dignify the omnipresent expression $C\tau + D$ with a name.

[34] Here we are (mildy) abusing notation by letting $\mathscr{L}_{j^k}(\Gamma)$ refer to both a line bundle and its sheaf of sections.

Definition 3.13. *Let Γ be an arithmetic subgroup of $Sp_{2g}(\mathbb{Q})$ for $g \geq 2$. A* **modular form** *of* **weight** *k ($k \in \mathbb{Z}$) for Γ is a holomorphic function $f : \mathbb{H}^g \to \mathbb{C}$ satisfying the functional equation*

$$f(\gamma\tau) = j_\gamma^k(\tau)f(\tau)$$

for all $\tau \in \mathbb{H}^g$ and all $\gamma \in \Gamma$;

Remark: When $g = 1$ we must also ask that f is "holomorphic at the cusps."[35] In fact, we also require that modular forms on $\mathbb{H}^g$ for $g > 1$ satisfy an analogous condition, but thankfully this turns out to be no condition at all when $g > 1$ as it is automatically satisfied by any holomorphic function satisfying definition 3.13 . This small mercy for expositors of the theory modular forms is known as **Köcher's principle.**

Definition 3.14. *A modular form $f \in M_k\big(Sp_{2g}(\mathbb{Z})\big)$ is called a* **cusp form** *if*

$$\lim_{t\to\infty} F\begin{pmatrix}\tau & 0\\ 0 & it\end{pmatrix} = 0$$

for all $\tau \in \mathbb{H}^{g-1}$. More generally, if Γ is an arithmetic subgroup of $Sp_{2g}(\mathbb{Q})$ then we say that $f \in M_k\big(\Gamma\big)$ is a cusp form if for all

$$\alpha = \begin{pmatrix}A & B\\ C & D\end{pmatrix} \in Sp_{2g}(\mathbb{Q})$$

and all $\tau \in \mathbb{H}^{g-1}$ we have

$$\lim_{t\to\infty} \det\big(C\begin{pmatrix}\tau & 0\\ 0 & it\end{pmatrix} + D\big)^{-k} f\Big(\alpha\begin{pmatrix}\tau & 0\\ 0 & it\end{pmatrix} = 0.$$

4 Hecke Algebras

4.1 Hecke Pairs and Hecke Algebras

One of the most elementary yet important results in group theory is that whenever one has a group G and a subgroup $\Gamma \subseteq G$ then the set of right (resp. left) cosets of Γ is a partition of G with an associated right (resp. left) permutation action by G. Hecke algebras – to be defined momentarily – appear in the context of another [36] partition of G which may be associated to Γ.

Definition 4.1. *A* **double coset** *of Γ in G is a set of the form*

$$\Gamma g\Gamma := \{\gamma_1 g\gamma_2 \mid \gamma_i \in \Gamma\}$$

where g is a fixed element of G.

Lemma 4.1. *G is partitioned by the double cosets of Γ.*

Proof. If $g, h \in G$ are such that $\gamma_1 g\gamma_2 = \gamma_3 h\gamma_4$ then $h = (\gamma_3^{-1}\gamma_1)g(\gamma_2\gamma_4^{-1})$ ie. $h \in \Gamma g\Gamma$. It follows that distinct double cosets are disjoint.

□

[35] See §1 for a definition of this condition in the "classical" notation.

[36] Equally natural if – admittedly – less elementary.

Corollary 4.1. *Every double coset $\Gamma g\Gamma$ is partitioned by left (equivalently right) cosets of Γ.*

Proof. A left coset $g\Gamma$ (resp. right coset Γg) is obviously contained in $\Gamma g\Gamma$ since the identity element of G belongs to Γ and so

$$\Gamma g\Gamma = \bigcup_{g'\Gamma\cap\Gamma g\Gamma\neq\varnothing} g'\Gamma = \bigcup_{\Gamma g''\cap\Gamma g\Gamma\neq\varnothing} \Gamma g''.$$

These unions are disjoint since distinct left (resp right) cosets of Γ are disjoint in G.

□

Definition 4.2. *The pair (G,Γ) is called a* **Hecke pair** *if every double coset of Γ in G is a finite union of left cosets (and thus also right cosets) of Γ in G.*

Henceforth (G,Γ) is assumed to be a Hecke pair.

Let $\mathbb{Z}[\Gamma\backslash G]$ denote the free abelian group on the right cosets of Γ in G. There is a natural right action of G on this space by $\mathbb{Z}$-linear automorphisms, the so-called **right regular representation**,[37] whereby $h \in G$ acts as

$$\Big(\sum_g \Gamma g\Big)h := \sum_g \Gamma(gh).$$

Let $\mathbb{Z}[\Gamma\backslash G]^\Gamma$ denote the submodule of Γ-invariants for this representation, ie.

$$\mathbb{Z}[\Gamma\backslash G]^\Gamma = \{X \in \mathbb{Z}[\Gamma\backslash G] \mid X\gamma = X \text{ for all } \gamma \in \Gamma\}.$$

Lemma 4.2. *Let $\mathbb{Z}[\Gamma]$ be the group ring of Γ and let $\mathbb{Z}[\Gamma\backslash G/\Gamma]$ be the free abelian group on the double cosets of Γ. Let $\eta : \Gamma\backslash G/\Gamma \to \mathbb{Z}[\Gamma\backslash G]$ be the function*

$$\eta(\Gamma g\Gamma) := \sum_{g'\in\Gamma\backslash\Gamma g\Gamma} \Gamma g'$$

and extend η in the unique way to a $\mathbb{Z}$-linear map defined on $\mathbb{Z}[\Gamma\backslash G/\Gamma]$. Then η is an isomorphism of (right) $\mathbb{Z}[\Gamma]$ modules between $\mathbb{Z}[\Gamma\backslash G/\Gamma]$ and $\mathbb{Z}[\Gamma\backslash G]^\Gamma$.

Proof. We begin by remarking that η is well defined: for each $g \in G$, $\gamma \in \Gamma$ descends via the right regular representation to a well defined permutation of the set of right cosets of Γ in $\Gamma g\Gamma$, and $\eta(\Gamma g\Gamma)$ is independent of the choice of representatives g' for the right cosets since these are unique up to left translations by Γ.

Given what has just now been remarked, $\eta(\Gamma g\Gamma)$ is certainly Γ invariant on the right, and η is injective since distinct double cosets of Γ are disjoint in G. As for surjectivity, if

$$X = \sum_{\Gamma g\in\Gamma\backslash G} a_{\Gamma g}\Gamma g \quad (a_{\Gamma g} \in \mathbb{Z} \text{ is zero for all but finitely many } \Gamma g)$$

is right Γ invariant then the coefficients $a_{\Gamma g}$ are themselves right Γ invariant in the sense that $a_{\Gamma g\gamma} = a_{\Gamma g}$ for all $\Gamma g, \gamma$. Then defining $a_{\Gamma g\Gamma} := a_{\Gamma g}$ we have

$$X = \sum_{\Gamma g\Gamma\in\Gamma\backslash G/\Gamma} a_{\Gamma g\Gamma} \sum_{\Gamma g'\in\Gamma\backslash\Gamma g\Gamma} \Gamma g' = \eta\Big(\sum_{\Gamma g\Gamma\in\Gamma\backslash G/\Gamma} a_{\Gamma g\Gamma}\Gamma g\Gamma\Big).$$

[37] This is the induced representation $\mathrm{Ind}\uparrow_\Gamma^G \mathbb{Z}$ where $\mathbb{Z}$ is equipped with a trivial action of Γ.

□

To each double coset $\Gamma g \Gamma$ we associate a linear endomorphism $T_{\Gamma g \Gamma}$ of $\mathbb{Z}[\Gamma \backslash G]$ by defining

$$T_{\Gamma g \Gamma}(\Gamma h) := \sum_{\Gamma g' \in \Gamma g \Gamma} \Gamma(g'h)$$

for right cosets Γh and extending linearly. We remark that this definition does not depend upon the choice of representative elements g' for the right cosets of Γ in $\Gamma g \Gamma$ (which are uniquely defined up to left translation by Γ), nor on the choice of representative for the right coset Γh, since if we replace h with γh then

$$\begin{aligned} T_{\Gamma g \Gamma}(\Gamma \gamma h) &= \sum_{\Gamma g' \in \Gamma g \Gamma} \Gamma(g' \gamma h) \\ &= \Big(\sum_{\Gamma g' \in \Gamma g \Gamma} \Gamma g' \Big) \gamma h \\ &= \eta(\Gamma g \Gamma) \gamma h \\ &= \eta(\Gamma g \Gamma) h && \text{since } \eta(\Gamma g \Gamma) \in \mathbb{Z}[\Gamma \backslash G]^{\Gamma} \\ &= \Big(\sum_{\Gamma g' \in \Gamma g \Gamma} \Gamma(g') \Big) h \\ &= \sum_{\Gamma g' \in \Gamma g \Gamma} \Gamma(g'h). \end{aligned}$$

Lemma 4.3. *Each $T_{\Gamma g \Gamma}$ restricts to an endomorphism of $\mathbb{Z}[\Gamma \backslash G]^{\Gamma}$.*

Proof. This will follow immediately if we know that each $T_{\Gamma g \Gamma}$ commutes with the right regular representation of G on $\mathbb{Z}[\Gamma \backslash G]$. As for this latter claim, for each right coset Γh and each $g'' \in G$ we have

$$\big(T_{\Gamma g \Gamma}(\Gamma h)\big) g'' = \Big(\sum_{\Gamma g' \in \Gamma \backslash \Gamma g \Gamma} \Gamma(g'h) \Big) g'' = \Big(\sum_{\Gamma g' \in \Gamma \backslash \Gamma g \Gamma} \Gamma(g' h g'') \Big) = T_{\Gamma g \Gamma}(\Gamma h g'').$$

Thus the two linear actions commute on each canonical basis element and so also as operators on $\mathbb{Z}[\Gamma \backslash G]$.

□

Definition 4.3. *Let (G, Γ) be a Hecke pair. The* **Hecke ring** *$\mathcal{H}(G, \Gamma)$ of the pair is the ring whose underlying abelian group is the double coset space $\mathbb{Z}[\Gamma \backslash G / \Gamma]$ and whose product (denoted by $*$) is defined on basis elements by*

$$\Gamma g \Gamma * \Gamma h \Gamma := \eta^{-1}\big(T_{\Gamma g \Gamma}(\eta(\Gamma h \Gamma))\big)$$

.

Remark:

- The binary operation $*$ is associative. Observe that $\eta(\Gamma h \Gamma) = T_{\Gamma h \Gamma}(\Gamma)$ where $\Gamma = \eta(\Gamma 1 \Gamma)$ is the right (equivalently double) coset of the identity in G. We can thus write $\Gamma g \Gamma * \Gamma h \Gamma := \eta^{-1}\big(T_{\Gamma g \Gamma} \circ T_{\Gamma h \Gamma}(\Gamma)\big)$ whence associativity follows as composition of functions is always associative.

- We may replace $\mathbb{Z}$ with any commutative coefficient ring R and speak instead of the **Hecke algebra** $\mathcal{H}(G, \Gamma) \otimes R$ over R.

Proposition 4.1. *Let V be vector space over a field K and let $\rho : G \to GL(V)$ be a K-linear representation. Then ρ induces a $\mathcal{H}(G,\Gamma) \otimes K$ module structure on the subspace $V^\Gamma := \{v \in V \mid \rho(\gamma)v = v \text{ for all } \gamma \in \Gamma\}$ of Γ-invariant vectors in V.*

Proof. For each double coset $\Gamma g \Gamma = \bigsqcup_{g'} \Gamma g'$ and each $v \in V^\Gamma$ we define

$$\rho_{\mathcal{H}}(\Gamma g \Gamma)v := \sum_{g'} \rho(g')v.$$

and extend this K-linearly to all linear combinations of double cosets. Each of these operators preserves V^Γ since whenever $\gamma \in \Gamma$ we have $\Gamma g \Gamma = \bigsqcup_g' \Gamma g'$ if and only if $\Gamma g \Gamma = \bigsqcup_g' \Gamma \gamma^{-1} g'$, in which case

$$\rho(\gamma)\rho_{\mathcal{H}}(\Gamma g \Gamma)v = \rho(\gamma)\sum_{g'} \rho(\gamma^{-1}g')v = \sum_{g'} \rho(\gamma\gamma^{-1}g')v = \sum_{g'} \rho(g')v = \rho_{\mathcal{H}}(\Gamma g \Gamma)v.$$

Since the identity element in the Hecke algebra is the double coset of the identity in G (ie. Γ itself) we have $\rho_{\mathcal{H}}(id_{\mathcal{H}(G,\Gamma)\otimes K}) = id_{V^\Gamma}$. Given an arbitrary pair of double cosets $\Gamma g \Gamma, \Gamma h \Gamma$ we have

$$\begin{aligned} \rho_{\mathcal{H}}(\Gamma g \Gamma) \circ \rho_{\mathcal{H}}(\Gamma h \Gamma)v &= \rho(\Gamma g \Gamma)\Big(\sum_{h'} \rho(h')v\Big) \\ &= \sum_{g',h'} \rho(g'h')v. \end{aligned}$$

On the other hand, notice that the action of any given double coset $\Gamma u \Gamma$ "factors through" the K linear isomorphism $\eta : K[\Gamma\backslash G/\Gamma] \xrightarrow{\sim} K[\Gamma\backslash G]^\Gamma$ upon choosing an arbitrary set of representatives u' in G for each right coset in the sum $\eta(\Gamma u \Gamma) = \sum_{\Gamma u' \in \Gamma\backslash\Gamma u \Gamma} \Gamma u'$ and defining $\rho_{\mathcal{H}}(\Gamma u \Gamma)v = \sum_{u'} \rho(u')v$. Given this, we compute

$$\eta(\Gamma g \Gamma * \Gamma h \Gamma) = T_{\Gamma g \Gamma}(\sum_{h'} \Gamma h') := \sum_{g'}\sum_{h'} \Gamma g'h'$$

whence it follows that

$$\rho_{\mathcal{H}}(\Gamma g \Gamma * \Gamma h \Gamma) = \rho_{\mathcal{H}}(\Gamma g \Gamma) \circ \rho_{\mathcal{H}}(\Gamma h \Gamma)$$

for all double cosets $\Gamma g \Gamma, \Gamma h \Gamma$. Since the entire algebra structure of the Hecke algebra is determined on its basis of double cosets we conclude that $\rho_{\mathfrak{H}} : \mathcal{H}(G,\Gamma) \otimes K \to \mathrm{End}_K(V^\Gamma)$ is a well defined homomorphism of K-algebras.

□

4.2 Hecke algebras acting on modular forms

Let $\mathrm{GSp}_{2g}^+(\mathbb{Q}) := \{g \in \mathrm{GSp}_{2g}(\mathbb{Q}) \mid \det g > 0\}$. Our starting point is the following theorem:

Theorem 17. *For all integers $g \geq 1$ and all congruence subgroups $\Gamma \subseteq Sp_{2g}(\mathbb{Q})$ the pair $\big(GSp_{2g}^+(\mathbb{Q}), \Gamma)\big)$ is a Hecke pair.*

Proof. See [A-Z, Chap. 3, Lemma 3.1].

□

Let $\mathcal{O}(\mathbb{H}^g)$ denote the vector space of all holomorphic functions $f : \mathbb{H}^g \to \mathbb{C}$. For each integer k and each $g \in \mathrm{GSp}_{2g}^+(\mathbb{Q})$ we define the **slash operator** of weight k for g to be the following linear operator on $\mathcal{O}(\mathbb{H}^g)$:

$$\big(\phi|_k g\big)(\tau) := \det(\gamma)^{k-1}\det(C\tau+D)^{-k}\phi(\gamma\tau)$$

where $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ acts on $\mathbb{H}^g$ as in §3.

Lemma 4.4. *For each $k \in \mathbb{Z}$, the function*

$$GSp_{2g}^+(\mathbb{Q}) \to GL(\mathcal{O}(\mathbb{H}^g)), \quad g \mapsto |_k g$$

is a linear representation.

Proof. The $2g \times 2g$ identity matrix clearly maps to the identity operator for any k. Fixing k and letting **(i)** $g, g' \in \mathrm{GSp}_{2g}^+(\mathbb{Q})$,**(ii)** $\phi \in \mathcal{O}(\mathbb{H}^g)$ and **(iii)** $\tau \in \mathbb{H}^g$ be arbitrary we have

$$\begin{aligned}
\big(\phi|_k g|_k g'\big)(\tau) &:= \det(g')^{k-1}\det(C'\tau+D')^{-k}\big(\phi|_k g\big)(\gamma'\tau) \\
&:= \det(g')^{k-1}\det(g)^{k-1}\det(C'\tau+D')^{-k} \\
&\quad \times \det\big(C(A'\tau+B')(C'\tau+D')^{-1}+D\big)^{-k}\phi(\gamma\gamma'\tau) \\
&= \det(gg')^{k^{-1}}\det\big((CA'+DC')\tau+CB'+DD')\big)^{-k}\phi(\gamma\gamma'\tau) \\
&= \big(\phi|_k gg'\big)(\tau)
\end{aligned}$$

where the final line follows because

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} = \begin{pmatrix} AA'+BC' & AB'+BD' \\ CA'+DC' & CB'+DD' \end{pmatrix}.$$

□

By construction, for any discrete subgroup Γ of $\mathrm{Sp}_{2g}(\mathbb{Q})$ the slash operators give an alternative characterisation of the space of modular forms of weight k with respect to Γ, namely

$$M_k(\Gamma) = \{\phi \in \mathcal{O}(\mathbb{H}^g) \mid \phi|_k\gamma = \phi \text{ for all } \gamma \in \Gamma\} = \mathcal{O}(\mathbb{H}^g)^{|_k\Gamma}.$$

Combining this with theorem refheckepair and proposition 4.1 we obtain the following theorem:

Theorem 18. *For each congruence subgroup Γ of $Sp_{2g}(\mathbb{Q})$ the algebra $M_*(\Gamma) = \oplus_{k\in\mathbb{Z}} M_k(\Gamma)$ of modular forms with respect to Γ is a graded module over the Hecke algebra $\mathcal{H}(GSp_{2g}^+(\mathbb{Q}), \Gamma)$.*

Example 4.1.

Recall that when $g =$ we can identify $\mathrm{GSp}_{2g}^{+}(\mathbb{Q}) \cong$ with $\mathrm{GL}_2^{+}(\mathbb{Q})$ and $\mathrm{Sp}_2(\mathbb{Z})$ with $\mathrm{SL}_2(\mathbb{Z})$. The set

$$\{A \in \mathrm{GL}_2(\mathbb{Z}) \mid \det A = p\}$$

comprises one double coset of $\mathrm{SL}_2(\mathbb{Z})$ in $\mathrm{GL}_2(\mathbb{Q})$ with right coset representatives

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \text{ for } 0 \le b \le p-1.$$

The double coset $\mathrm{SL}_2(\mathbb{Z})\mathrm{diag}(p,1)\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{O}(\mathbb{H}^1)$ via the weight k slash operator according to the rule

$$\begin{aligned} \big(f|_k\mathrm{SL}_2(\mathbb{Z})\mathrm{diag}(p,1)\mathrm{SL}_2(\mathbb{Z})\big)(\tau) &= \big(f|_k\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\big)(\tau) + \sum_{b=0}^{p-1}\big(f|_k\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}\big)(\tau) \\ &= p^{k-1}\Big(f(p\tau) + \frac{1}{p^k}\sum_{b=0}^{p-1} f\big(\frac{\tau+b}{p}\big)\Big) \\ &= p^{k-1}f(p\tau) + \frac{1}{p}\sum_{b=0}^{p-1} f\big(\frac{\tau+b}{p}\big) \end{aligned}$$

Thus if f is a modular form of weight k with Fourier development $f(\tau) = \sum_{n\ge0} a_n q^n$ where $q = e^{2\pi i\tau}$ then

$$\begin{aligned} \big(f|_k\mathrm{SL}_2(\mathbb{Z})\mathrm{diag}(p,1)\mathrm{SL}_2(\mathbb{Z})\big)(\tau) &= p^{k-1}f(p\tau) + \frac{1}{p}\sum_{b=0}^{p-1} f\big(\frac{\tau+b}{p}\big) \\ &= \sum_{n\ge0} p^{k-1}a_n q^{np} + \frac{1}{p}\sum_{b=0}^{p-1}\sum_{n\ge0} a_n e^{2\pi i\frac{n}{p}(\tau+b)} \\ &= \sum_{n\ge0} p^{k-1}a_n q^{np} + \frac{1}{p}\sum_{b=0}^{p-1}\sum_{n\ge0,\ p|n} a_n e^{2\pi i\frac{n}{p}(\tau+b)} \\ &= \sum_{n\ge0} p^{k-1}a_n q^{np} + \frac{1}{p}\sum_{b=0}^{p-1}\sum_{n\ge0} a_{np} q^n e^{2\pi ibn/p} \\ &= \sum_{n\ge0} p^{k-1}a_n q^{np} + \sum_{n\ge0} a_{np} q^n \end{aligned}$$

where in the second line we have used the fact that Hecke operators preserve the space of modular forms of a given weight and that every modular form has a Fourier development in non-negative integral powers of q. We have thus recovered the formula with which we defined the Hecke operator at p of weight k in §1.

For posterity, we record the action of this operator on Fourier coefficients.

Corollary 4.2. *For $f \in M_k(SL_2(\mathbb{Z})$ let $[f]_n$ denote the coefficient of q^n in the expansion of f and let. Then*

$$\Big[f|_k SL_2(\mathbb{Z})\,diag(p,1)\,SL_2(\mathbb{Z})\Big]_n = \begin{cases} [f]_{np}, & \textit{if } p \nmid n, \\ [f]_{np} + p^{k-1}[f]_{n/p}, & \textit{if } p \mid n. \end{cases}.$$

□

Lemma 4.5. *Let k be a postive integer and let p be a prime number. Let $f(q) = \sum_{n\geq 1} a_n q^n \in S_k(SL_2(\mathbb{Z})$ be an eigenvector of the Hecke operator $SL_2(\mathbb{Z})diag(p,1)SL_2(\mathbb{Z})$ with eigenvalue $\lambda(p)$. Then $\lambda(p)a_1 = a_p$.*

Proof. We have

$$\sum_{n\geq 1} \lambda(p) a_n q^n = \big(f|_k \mathrm{SL}_2(\mathbb{Z})\mathrm{diag}(p,1)\mathrm{SL}_2(\mathbb{Z})\big)(q) := \sum_{n\geq 0} p^{k-1} a_n q^{np} + \sum_{n\geq 0} a_{np} q^n$$

and the claimed identity follows upon equating the coefficients of q^1 in each series.

□

As a corollary we discover that the Fourier coefficients of simultaneous eigenvectors are multiplicative:

Corollary 4.3. *Let ℓ and p be distinct primes and suppose that $f = \sum_{n\geq 1} a_n q^n$ is a eigenvector for both $SL_2(\mathbb{Z})diag(p,1)SL_2(\mathbb{Z})$ and $SL_2(\mathbb{Z})diag(\ell,1)SL_2(\mathbb{Z})$. Then $a_{p\ell} = a_p a_\ell$.*

Proof. This is a straightforward computation. We omit the details.

□

4.3 Reductive groups, Maximal Tori and Weyl groups

Before we can say anything more about the structure of the Hecke algbebras $\mathcal{H}(\mathrm{GSp}_{2g}^+(\mathbb{Q}), \Gamma)$ we must first collect some definitions and theorems (without proof) from the theory of reductive groups.

Definition 4.4. *Let G be an algebraic group. An element $u \in G$ is called* **unipotent** *if for every faithful linear representation $\rho : G \hookrightarrow GL(V)$ on a finite dimensional vector space V there exists a positive integer n such that $(\rho(u) - id_V)^n = id_V$. An algebraic group U is called a* **unipotent group** *if every $u \in U$ is unipotent.*

Example 4.2.

The additive group $\mathbb{G}_a$ is a unipotent group.

Definition 4.5. *A* **reductive group** *is a geometrically connected*[38] *algebraic group which contains no non-trivial normal unipotent subgroups.*

Examples 4.1.

1. The multiplicative group $\mathbb{G}_m$ is reductive. More generally, $\mathbb{G}_m^n$ is reductive for all positive integers n.

2. The general linear groups GL_n and the special linear groups SL_n are all reductive.

3. The general symplectic group GSp_{2g} and its subgroup Sp_{2g} are both reductive.

[38] A variety V over a field K is **geometrically connected** if the base change of V to an algebraic closure of K is connected.

Definition 4.6. *Let $\mathcal{G}$ be a reductive group over a field K. A* **torus** *in $\mathcal{G}$ is a commutative subgroup T of $\mathcal{G}$ which is isomorphic (possibly over an extension of K) to a product $\mathbb{G}_m^n$ of multiplicative groups. A torus $T \cong \mathbb{G}_m^n$ is called a* **maximal torus** *if whenever $T' \cong \mathbb{G}_m^{n'}$ is another torus is $\mathcal{G}$ then $n' \leq n$.*

Examples 4.2.

Let R be a commutative ring.

1. A maximal torus for GL_n is the group scheme T_n whose group $T_n(R)$ of R-points is the subgroup of diagonal matrices in $\mathrm{GL}_n(R)$, ie.

$$T(R) = \{\mathrm{diag}(t_1, \ldots, t_n) \mid t_i \in R^\times\}.$$

Clearly $T \cong \mathbb{G}_m^n$

2. A maximal torus in SL_n is the group scheme $T_{n,1}$ whose R-points are n by n diagonal matrices with entries in R and determinant 1. Explicitly,

$$\begin{aligned} T_{n,1}(K) &= \{\mathrm{diag}(a_1, \ldots, a_n) \mid a_i \in K^\times, \prod_i a_i = 1\} \\ &= \{\mathrm{diag}(a_1, \ldots, a_{n-1}, \prod_{i=i}^{n-1} a_i^{-1}) \mid a_i \in K^\times\} \end{aligned}$$

This latter description shows that $T_{n,1} \cong \mathbb{G}_m^{n-1}$.

3. A maximal torus for GSp_{2g} is the subgroup scheme T whose set of R-points for each commutative ring R is the subgroup of diagonal matrices in $\mathrm{GSp}_{2g}(R)$, ie. matrices of the form

$$D := \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & & \\ & & a_g & & & \\ & & & b_1 & & \\ & & & & \ddots & \\ & & & & & b_g \end{pmatrix} \quad a_i, b_j \in R^\times$$

which satisfy $D^t J D = \lambda J$ for some constant $\lambda \in R^\times$. Since

$$D^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} D = \begin{pmatrix} & & & a_1 b_1 & & \\ & & & & \ddots & \\ & & & & & a_g b_g \\ -a_1 b_1 & & & & & \\ & \ddots & & & & \\ & & -a_g b_g & & & \end{pmatrix}$$

the condition is that

$$D = \begin{pmatrix} \mathrm{diag}(a_1, \ldots, a_g) & 0 \\ 0 & \lambda \mathrm{diag}(a_1^{-1}, \ldots, a_g^{-1}) \end{pmatrix}$$

for arbitrary $a_1, \ldots, a_g, \lambda \in R^\times$. It follows from this analysis that $T \cong \mathbb{G}_m^{g+1}$.

Theorem 19. *Every reductive group $\mathcal{G}$ has a maximal torus T. Moreover, any two maximal tori in $\mathcal{G}$ are conjugate.*

Proof. For general facts about reductive groups, see [Springer].

□

Definition 4.7. *Let $\mathcal{G}$ be a reductive group with maximal torus T and let N_T be the normalizer of T in $\mathcal{G}$. The* **Weyl group** *of $\mathcal{G}$ is the group $W_{\mathcal{G}} := N_T/T$.*

Examples 4.3.

1. The normalizer of T_n in GL_n is the group N_n of **generalised permutation matrices** ie. n by n matrices with a single non-zero entry in each row and column. Up to the action of the torus T_n on N_n we can assume that all non-zero entries are equal to 1, and in this way we identify W_{GL_n} with the group of n by n permutation matrices or, equivalently, with the symmetric group S_n on n letters.

2. The normalizer of $T_{n,1}$ in SL_n is the subgroup $N_{n,1}$ of N_n comprising generalised permutation matrices with determinant 1. If $A = \mathrm{diag}(a_1, \ldots, a_n) \in T_{n,1}(K)$ and $X \in N_{n,1}$ then
$$XAX^{-1} = \mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$$
for some permutation σ and all such permutations can be attained in this way. It follows that W_{SL_n} is once again isomorphic to the symmetric group S_n on n letters.

3. The Weyl group of GSp_{2g} is isomorphic to a semidirect product $S_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$ where S_g is the symmetric group on g letters [Van der Geer, §12, pg. 25]. A permutation $\sigma \in S_g$ acts on $T(R)$ as
$$\sigma \mathrm{diag}(a_1, \ldots, a_g, b_1, \ldots, b_g) := \mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(g)}, b_{\sigma(1)}, \ldots, b_{\sigma(g)})$$
and the i^{th} factor of $\mathbb{Z}/2\mathbb{Z}$ interchanges a_i and b_i.

4.4 Local Hecke Algebras

Let $\mathcal{G}$ be a reductive group. Then for each prime number p the group $G := \mathcal{G}(\mathbb{Q}_p)$ is a locally compact group. with maximal compact subgroup $K := \mathcal{G}(\mathbb{Z}_p)$. Let $d\mu$ be Haar measure on G normalised so as to give K unit mass ie. $\int_G \chi_K d\mu = 1$ where χ_K is the characteristic function of K.

Definition 4.8. *The* **(unramified) local Hecke algebra** *$\mathcal{H}(G, K)$ of G is the $\mathbb{C}$-vector space of all locally constant, K bi-invariant and compactly supported functions $f : G \to \mathbb{C}$ with the* **convolution product**
$$f * g(x) := \int_G f(xy)g(y^{-1})d\mu(y).$$

Lemma 4.6. *The convolution product is well defined and gives $\mathcal{H}(G, K)$ the structure of a associative and unital $\mathbb{C}$-algebra. That is,* *(a) Whenever $f, g : G \to \mathbb{C}$ are locally constant, compactly supported and K bi-invariant then $f * g$ also enjoys these properties;*

(b) $(f * g) * h = f * (g * h)$ for all $f, g, h \in \mathcal{H}(G, K)$;

(c) there exists an identity element in $\mathcal{H}(G, K)$ with respect to convolution.

Proof. So as to give a flavour of the method of proof we will prove the claims about K bi-invariance, compact support and the existence of a unit element.

For all $k \in K$ we have

$$f * g(kx) = \int_G f(kxy)g(y^{-1})d\mu(y) = \int_G f(xy)g(y^{-1})d\mu(y)$$

(since f is left K-invariant) and

$$f*g(xk) = \int_G f(xky)g(y^{-1})d\mu(y) = \int_G f(xky)g(y^{-1}k^{-1})d\mu(ky) = \int_G f(xz)g(z^{-1})d\mu(z) \ (z := ky)$$

(since g is right K-invariant and $d\mu$ is Haar measure). Thus $f * g$ is K bi-invariant.

If $x \in G$ belongs to the support $\text{supp}(f * g)$ of $f * g$ then by inspection of the convolution integral the set $\{y \in G \mid xy \in \text{supp}(f) \text{ and } y \in \text{supp}(g)^{-1}\}$ has positive measure. Let y be any element of this set. Then **(i)** $y = x^{-1}u$ for $u \in \text{supp}(f)$ and **(ii)** $y = v^{-1}$ for some $v \in \text{supp}(g)$. But then $v^{-1} = x^{-1}u$ or in other words $x = uv$. It follows that $\text{supp}(f * g) \subseteq \text{supp}(f)\text{supp}(g)$. This latter set is the image of the compact subset $\text{supp}(f) \times \text{supp}(g)$ of $G \times G$ under the continuous multiplication map $G \times G \to G$ it follows that $\text{supp}(f * g)$ is contained in a compact subset of G ie. $f * g$ is compactly supported.

Let χ_K denote the characteristic function of $K$and let $f \in \mathcal{H}(G, K)$ be arbitary. Then since$f$ is K bi-invariant and χ_K is supported on K we have

$$f * \chi_K(x) = \int_G f(xy)\chi_K(y^{-1})d\mu(y) = \int_K f(xy)\chi_K(y^{-1})d\mu(y) = f(x)\int_K d\mu = f(x)$$

and

$$\begin{aligned}
\chi_K * f(x) &= \int_G \chi_K(xy)f(y^{-1})d\mu(y) \\
&= \int_{x^{-1}K} \chi_K(xy)f(y^{-1})d\mu(y) \\
&= \int_{x^{-1}K} f(xyy^{-1})d\mu(y) \\
&= f(x)\int_{x^{-1}K} d\mu \\
&= f(x)
\end{aligned}$$

where in the third to last line we observe that $xy \in K$ for all $y \in x^{-1}K$ and in the last line we use that μ is a translation invariant measure. It follows that χ_K is an identity element with respect to $*$.

□

Remark: In the definition of the unramified local Hecke algebra, one may replace K with any open compact subgroup K' of G (while otherwise leaving the definitions untouched) to produce a variety of **ramified** local Hecke algebras $\mathcal{H}(G, K')$.

The study of local Hecke algebras is amply motivated by the following theorem.

Theorem 20. *There is an isomorphism*

$$\mathcal{H}(GSp^{+}(\mathbb{Q}), Sp_{2g}(\mathbb{Z})) \cong \bigotimes_{p} \mathcal{H}(GSp_{2g}(\mathbb{Q}_p), GSp_{2g}(\mathbb{Z}_p)).$$

More generally, if $\Gamma \subseteq Sp_{2g}(\mathbb{Z})$ *is a congruence subgroup then*

$$\mathcal{H}\big(GSp^{+}(\mathbb{Q}), \Gamma\big) \cong \bigotimes_{p} \mathcal{H}\big(GSp_{2g}(\mathbb{Q}_p), K_p)\big)$$

where K_p *is an open compact subgroup of* $GSp_{2g}(\mathbb{Z}_p)$ *with* $K_p = GSp_{2g}(\mathbb{Z}_p)$ *for all but finitely many primes* p.

Proof. See [Van der Geer, §16, page 30].

□

Remark: Though we omit the proof of theorem 20, we remark that the subalgebra of $\mathcal{H}(\mathrm{GSp}^{+}(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z}))$ corresponding to $\mathcal{H}(\mathrm{GSp}(\mathbb{Q}_p), \mathrm{Sp}_{2g}(\mathbb{Z}_p))$ can be identified with the Hecke algebra of the pair

$$\Big(\mathrm{GL}_2(\mathbb{Z}[\frac{1}{p}])\, , \, \mathrm{SL}_2(\mathbb{Z}))\Big).$$

In other words, the unramified local Hecke algebra at p is isomorphic to the subalgebra of $\mathcal{H}(\mathrm{GSp}^{+}(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z}))$ generated by double cosets whose elements are integral up to p-power denominators.

An important step towards understanding the local Hecke algebras of GSp_{2g} is understanding the local Hecke algebras of its maximal torus T. Recall that any p-adic number x can be written uniquely in the form $x = p^{\nu_p(x)}u$ where ν_p is the p-adic valuation and $u \in \mathbb{Z}_p^{\times}$. We arrive at the following refined description of $T(\mathbb{Q}_p)$: it is the set of all matrices of the form

$$\begin{pmatrix} p^{t_1}u_1 & & & & & \\ & \ddots & & & & \\ & & p^{t_g}u_g & & & \\ & & & p^{\lambda}vp^{-t_1}u_1^{-1} & & \\ & & & & \ddots & \\ & & & & & p^{\lambda}vp^{-t_g}u_g^{-1} \end{pmatrix} \qquad t_1, \ldots, t_g, \lambda \in \mathbb{Z}, u, v \in \mathbb{Z}_p^{\times}.$$

If we define matrices

$$T_0(p) := \begin{pmatrix} I & 0 \\ 0 & pI \end{pmatrix}$$

and $T_i(p)$ for $i = 1, \ldots, g$ by

$$T_i(p) = \mathrm{diag}(t_i(1), \ldots, t_I(g), t_i(1)^{-1}, \ldots, t_i(g)^{-1})$$

where

$$t_i(j) := \begin{cases} 1, & \text{if } j \neq i, \\ p, & \text{if } j = i \end{cases}$$

ie.

$$T_1(p) := \begin{pmatrix} p &&&&&&& \\ & 1 &&&&&& \\ && \ddots &&&&& \\ &&& 1 &&&& \\ &&&& p^{-1} &&& \\ &&&&& 1 && \\ &&&&&& \ddots & \\ &&&&&&& 1 \end{pmatrix}, \quad \ldots \quad T_g(p) := \begin{pmatrix} 1 &&&&&&&& \\ & \ddots &&&&&&& \\ && 1 &&&&&& \\ &&& p &&&&& \\ &&&& 1 &&&& \\ &&&&& \ddots &&& \\ &&&&&& 1 && \\ &&&&&&& p^{-1} & \end{pmatrix}$$

then every element X of $T(\mathbb{Q}_p)$ can be written uniquely in the form $X = U \prod_{i=0}^{g} T_i(p)^{n_i}$ with $U \in T(\mathbb{Z}_p)$ and $n_0, \ldots, n_g \in \mathbb{Z}$.

Lemma 4.7. *For $i = 0, \ldots, g$ let χ_i denote the characteristic function of the $T(\mathbb{Z}_p)T_i(p)T(\mathbb{Z}_p) = T_i(p)T(\mathbb{Z}_p) = T(\mathbb{Z}_p)T_i(p) \subseteq T(\mathbb{Q}_p)$.*[39] *Then $\chi_i * \chi = \chi_{ij}$ where χ_{ij} is the characteristic function of the coset $T(\mathbb{Z}_p)T_i(p)T_j(p)$.*

Proof. We have already shown (see lemma 4.6) that the support of $\chi_i * \chi_j$ must be a subset of $T(\mathbb{Z}_p)T_i(p)T_j(p)$. On the other hand , if $x = uT_i(p)T_j(p)$ for some $u \in T(\mathbb{Z}_p)$ then

$$\begin{aligned} \chi_i * \chi_j(x) &= \int_{t \in T(\mathbb{Q}_p)} \chi_i(uT_i(p)T_j(p)y)\chi_j(y^{-1})d\mu(y) \\ &= \int_{y \in T_j(p)^{-1}T(\mathbb{Z}_p)} \chi_i(uT_i(p)T_j(p)y)\chi_j(y^{-1})d\mu(y) \\ &= \int_{u' \in T(\mathbb{Z}_p)} \chi_i(uT_i(p)T_j(p)T_j(p)^{-1}u')\chi_j(u'T_j(p))d\mu(u') \\ &= \int_{u' \in T(\mathbb{Z}_p)} \chi_i(T_i(p))\chi_j(T_j(p))d\mu(u') \\ &= \int_{T(\mathbb{Z}_p)} d\mu \\ &= 1 \end{aligned}$$

where in the second line we have observed that $\chi_j(y^{-1}) \neq 0$ precisely when $y \in T_j(p)^{-1}T(\mathbb{Z}_p)$.

□

We have just proved

Theorem 21. *The unramified local Hecke algebra of the maximal torus T of $GSp_{2g}(\mathbb{Q}_p)$ is isomorphic to a ring of Laurent polynomials. Explicitly,*

$$\mathcal{H}\big(T(\mathbb{Q}_p), T(\mathbb{Z}_p)\big) = \mathbb{C}[\chi_0^{\pm}, \ldots, \chi_g^{\pm}].$$

[39] We remark that, as T is an commutative group, every double coset in T is really a single coset and $tT(\mathbb{Z}_p) = T(\mathbb{Z}_p)t$ for all $t \in T(\mathbb{Q}_p)$. We shall make use of this in the proof of the lemma.

□

For any reductive group G with maximal torus T_G and for any prime number p the action of the Weyl group W_G on $T_G(\mathbb{Q}_p)$ preserves $T_G(\mathbb{Z}_p)$, and so there is an induced action of W_G on $\mathcal{H}\big(T_G(\mathbb{Q}_p), T_G(\mathbb{Z}_p)\big)$.

Theorem 22. *(***The Satake Isomorphism)**
Let G be a reductive group with maximal torus T_G and corresponding Weyl group W_G. Then the unramified local Hecke algebra at p of G is isomorphic to the algebra of W_G invariants in the unramified local Hecke algebra of T_G, ie.

$$\mathcal{H}\big(G(\mathbb{Q}_p), G(\mathbb{Z}_p)\big) \cong \mathcal{H}\big(T_G(\mathbb{Q}_p), T_G(\mathbb{Z}_p)\big)^{W_G}.$$

Proof. See [Van der Geer, §17].

□

Corollary 4.4. *(a)*

$$\mathcal{H}\big(GSp_{2g}(\mathbb{Q}_p), GSp_{2g}(\mathbb{Z}_p)\big) \cong \mathbb{C}[\chi_0^{\pm}, \dots, \chi_g^{\pm}]^{S_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g}$$

where S_g acts by permuting $X_1, \dots, X_g$ and the i^{th} copy of $\mathbb{Z}/2\mathbb{Z}$ acts by inverting X_i.

(b) $\mathcal{H}\big(GSp_{2g}(\mathbb{Q}_p), GSp_{2g}(\mathbb{Z}_p)\big)$ is a commutative algebra.

□

Using the Satake isomorphism and the tensor product isomorphism (theorem 20) one can write down explicit generators for $\mathcal{H}(\mathrm{GSp}_{2g}^{+}(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z}))$.

Theorem 23. *The Hecke algebra $\mathcal{H}(GSp_{2g}^{+}(\mathbb{Q}), Sp_{2g}(\mathbb{Z})$ is generated by the double cosets of*

$$T(p) := \begin{pmatrix} I_g & 0 \\ 0 & pIg \end{pmatrix},$$

$$T(p)^{-1} := \begin{pmatrix} I_g & 0 \\ 0 & p^{-1}Ig \end{pmatrix},$$

and

$$T_i(p^2) := \begin{pmatrix} I_{g-i} & & & \\ & pI_i & & \\ & & p^2 I_{g-i} & \\ & & & pI_i \end{pmatrix}$$

as p runs over the set of prime numbers (I_j denotes the j by j identity matrix).

Proof. See [Van der Geer, §16, theorem 16.3] for a discussion and [A-Z] for a proof.

□

As was true for $g = 1$, for each weight k and each postive integer there exists a certain Hermitian product

$$S_k\big(\mathrm{Sp}_{2g}(\mathbb{Z})\big) \times S_k\big(\mathrm{Sp}_{2g}(\mathbb{Z})\big) \to \mathbb{C}$$

called the *Petersson product*[40] with respect to which the Hecke operators on $S_k\big(\mathrm{Sp}_{2g}(\mathbb{Z})\big)$ are all self adjoint. Since a family of self-adjoint commuting operators on a finite dimensional vector space can always be simultaneously diagonalised, we obtain the following startling theorem.

Theorem 24. *The space $S_k\big(Sp_{2g}(\mathbb{Z})\big)$ of cuspforms of weight k has a basis of simultaneous eigenvectors with respect to the Hecke algebra $\mathcal{H}\big(GSp_{2g}^+(\mathbb{Q}), Sp_{2g}(\mathbb{Z})\big)$.*

We are moved to make the following definition:

Definition 4.9. *Let Γ be an arithmetic subgroup of $Sp_{2g}(\mathbb{Q})\big)$. A* **Hecke eigenform** *for Γ is a modular form F which is a simultaneous eigenvector for the Hecke algebra $\mathcal{H}\big(GSp_{2g}^+(\mathbb{Q}), \Gamma\big)$.*

4.5 The L-series on a Hecke eigenform

Suppose that $F \in M_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ is a Hecke eigenform. Then the function

$$\mathcal{H}\big(\mathrm{GSp}_{2g}^+(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z})\big) \to \mathbb{C}$$

which sends a Hecke operator ϕ to its eigenvalue on $\mathbb{C}$-span$\{F\} \subseteq M_k(\mathrm{Sp}_{2g}(\mathbb{Z})\big)$ is a complex character (ie. a $\mathbb{C}$-algebra homomorphism with 1-dimensional image) of the Hecke algebra. We denote this **Hecke character** by χ_F. For all primes p we obtain a character $\chi_{F,p}$ of the unramified local Hecke algebra at p as the composition

$$\mathcal{H}(\mathrm{GSp}_{2g}(\mathbb{Q}_p), \mathrm{GSp}_{2g}(\mathbb{Z}_p) \hookrightarrow \bigotimes_p \mathcal{H}(\mathrm{GSp}_{2g}(\mathbb{Q}_p), \mathrm{GSp}_{2g}(\mathbb{Z}_p) \xrightarrow{\sim} \mathcal{H}(\mathrm{GSp}_{2g}^+(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z}) \xrightarrow{\chi_F} \mathbb{C}$$

which we may identify with a homomorphism of $\mathbb{C}$-algebras $\chi_{F,p} : \mathbb{C}[X_0^\pm, X_1^\pm, \ldots, X_g^\pm]^W \to \mathbb{C}$ where $W \cong S_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$ is the Weyl group of GSp_{2g} acting as in the preceding section. Tautologically, we have

$$\mathrm{Hom}_{\mathbb{C}\text{-alg}}\big(\mathbb{C}[X_0^\pm, X_1^\pm, \ldots, X_g^\pm]^W, \mathbb{C}\big) = (\mathbb{C}^\times)^{g+1}/W$$

and so we further identify $\chi_{F,p}$ with the W-orbit of a certain $(g+1)$-tuple $(\alpha_0, \ldots, \alpha_g)$ of non-zero complex numbers.

Definition 4.10. *With all notation being as above, a set of* **Satake parameters** *for F at p is any member of the W-orbit of $(\alpha_0, \ldots, \alpha_g)$.*

Definition 4.11. *Let $F \in S_k(Sp_{2g}(\mathbb{Z}))$ be a cuspidal Hecke eigenform. The* **(formal) spinor Euler factor** *of F at p is the expression*

$$L_p(F, spin, X) := (1 - \alpha_0 X) \prod_{r=1}^{g} \prod_{1 \le i_1 < \ldots < i_r \le g} (1 - \alpha_0 \alpha_1 \ldots \alpha_g X)$$

for any[41] *set of Satake parameters $(\alpha_0, \alpha_1, \ldots, \alpha_g)$ for F at p.*

The **(formal) spinor L-series** *of F is the infinite product*

$$L_{spin}(F, s) := \prod_p L_p(F, spin, p^{-s})^{-1}.$$

[40] We decline to give the definition (which can be found in [Van der Geer, §5] and [Andrianov, §1.3 (especially theorem 1.38)]) simply because we will not revisit this product again after the present paragraph.

[41] Since Satake parameters are unique up to conjugacy this is well defined.

Remark: On the origin of the name "spinor." In the context of Langlands's theory of dual groups and L-groups the set of complex characters of $\mathcal{H}\big(\mathrm{GSp}_{2g}(\mathbb{Q}_p), \mathrm{GSp}(\mathbb{Z}_p)\big)$ is in canonical correspondence with the set of "semisimple" conjugacy classes (ie. conjugacy classes of points in the maximal torus) in a certain complex reductive Lie group $\mathrm{GSpin}_{2g+1}(\mathbb{C})$ which is related to the general symplectic group by $\mathrm{GSpin}_{2g+1} = \widehat{\mathrm{GSp}_{2g}}$ where $\widehat{\cdot}$ denotes the dual group construction. The local Hecke-character $\chi_{F,p}$ is thus identified with a conjugacy class $c_{F,p} \subseteq \mathrm{GSpin}_{2g+1}(\mathbb{C})$. To each irreducible and finite dimensional complex representation $\pi : \mathrm{GSpin}_{2g+1}(\mathbb{C}) \to \mathrm{GL}(V)$ we associate an Euler factor

$$L_p(F, \pi, X) := \det\big(1 - pi(c_{F,p})X|V\big)$$

and a corresponding (formal) L-series

$$L_\pi(F, s) := \prod_p L_p(F, \pi, p^{-s})^{-1}.$$

The spinor L-function corresponds to a certain $(2g+1)$-dimensional representation of $\mathrm{GSpin}_{2n+1}(\mathbb{C})$ occurring in the context of Clifford algebras and mathematical physic. Elements of the corresponding representation space are known as "spinors," whence the name.

4.6 Example: the spinor L-function of cuspform of level $\mathbf{SL}_2(\mathbb{Z})$.

The reasons for presenting the example in this section are twofold. Firstly, we hope to explain why the spinor L-series has been singled out for special attention, and secondly we wish to (finally!) find our way home to the basic motivating question of this thesis: just what should a Taniyama-Shimura-Weil / modularity conjecture look like when $g > 1$?

We begin by quoting three theorems. The first (respectively second) of which expresses the eigenvalues of a Hecke eigenform for $\mathrm{Sp}_{2g}(\mathbb{Z})$ (respecitvely the weight of a cuspidal Hecke eigenform for $\mathrm{SL}_2(\mathbb{Z})$) in terms of Satake parameters, and the third is the famous ramanujan identity for Hecke operators acting on $S_k(\mathrm{SL}_2(\mathbb{Z})$.

Theorem 25. *Let F be a Hecke eigenform for $Sp_{2g}(\mathbb{Z})$, let p be a prime number and let $(\alpha_0, \ldots, \alpha_g)$ be a set of Satake parameters for F at p. Let $\lambda(p)$ be the eigenvalue of F under the Hecke operator $T(p)$ (see theorem 23). For $j = 1$ to g let σ_j be the j^{th} elementary symmetric function in g variables evaluated at $(\alpha_1, \ldots, \alpha_g)$, ie.*

$$\sigma_j := \sum_{1 \le i_1 < i_2 < \ldots < i_j \le g} \alpha_{i_1}\alpha_{i_2} \ldots \alpha_{i_j}.$$

Then we have the identity

$$\lambda(p) = \alpha_0\big(1 + \sum_{j=1}^{g} \sigma_j\big).$$

Proof. This can derived from [A-Z, pages 142-145]. See [Van der Geer, §18 proposition 18.1 and §19] for a discussion.

□

Theorem 26. *Let p be a prime number, let $f \in S_k\big(SL_2(\mathbb{Z})\big)$ be a Hecke eigenform and let (α_0, α_1) be a set of Satake parameters for f at p. Then $\alpha_0^2\alpha^1 = p^{k-1}$.*

Proof. See [Van der Geer, §19] .

□

Before quoting the third theorem we remark that for each prime p and integer r the set $\mathrm{SL}_2(\mathbb{Q})[p^r] := \{A \in \mathrm{SL}_2(\mathbb{Q}) \mid \det(A) = p^r\}$ is – since the value of the determinant mapping is constant on any double coset of $\mathrm{SL}_2(\mathbb{Z})$ – a union of double cosets of $\mathrm{SL}_2(\mathbb{Z})$ and thus also a sum of Hecke operators. We denote this "total Hecke operator of $\mathrm{SL}_2(\mathbb{Q})[p^r]$" by $T(p^r)$.

Theorem 27. *For all primes numbers p and all integers $r > 1$ we have the identity*

$$T(p^{r+1}) = T(p)T(p^r) - p^{k-1}T(p^{r-1})$$

as operators on $M_2(SL_k(\mathbb{Z})$.

Proof. See [Zagier 123, §4 (especially 4.2)]

□

The result we are aiming for follows from these via a chain of corollaries.

Corollary 4.5. *Let $f = \sum_{n\geq 1} a_n q^n \in S_k\big(SL_2(\mathbb{Z})\big)$ wih $a_1 = 1$ and let $\lambda(p^r)$ denote the eigenvalue of f under the operator $T(p^r)$. Then for all primes p and all integers $r \geq 2$ we have $a_{pr} = \lambda(p^r)$.*

Proof. The case $r = 1$ is lemma 4.5. For $r = 2$, if for each modular form g we define $[g]_n$ to be the coefficient of q^n in the Fourier expansion of g then we combine theorem 27 and the explicit formula 4.2 for the action of $T(p)$ on Fourier coefficients to obtain

$$\lambda(p^2) = [T(p^2)f]_1 = [T(p)T(p)f]_1 - p^{k-1} = [f]_{np^2} + p^{k-1} - p^{k-1} = [f]_{np^2}.$$

The claim for general $r \geq 2$ now follows by induction from the base cases $r = 1, 2$ with a liberal use of theorem 27 and corollary 4.2.

□

Corollary 4.6. *Let $f = \sum_{n\geq 1} a_n q^n \in S_k(SL_2(\mathbb{Z})$ be a Hecke eigenform. Then the Euler factor for the spin L-series of f at p is*

$$L_p(f, spin, X) = \frac{1}{1 - a_p X + p^{k-1}X^2}.$$

Proof. From the definition of the spinor Euler factor at p we have

$$L_p(f, \mathrm{spin}, X) = \frac{1}{(1 - \alpha_0 X)(1 - \alpha_0\alpha_1 X)} = \frac{1}{1 - \alpha_0(1 + \alpha_1)X - \alpha_0^2\alpha_1 X}$$

and this is equal to $(1 - a_p X + p^{k-1}X^2)^{-1}$ by theorem 26.

□

Corollary 4.7. *Define*

$$\Phi_p(X) := 1 + \sum_{r\geq 1} T(p^r)X^r.$$

Then the identity

$$\Phi_p(X) = \big(1 - T(p)X + p^{k-1}X^2\big)^{-1}$$

holds in the ring $End_{\mathbb{C}}\big(M_k(SL_2(\mathbb{Z})\big)[[X]]$ *of formal power series over the endomorphism algebra of* $M_k\big(SL_2(\mathbb{Z})\big)$.

Proof. For convenience we define $T(p^0) = 1$. Then

$$\begin{aligned} & \big(1 - T(p)X + p^{k-1}X^2\big)\Phi_p(X) \\ = \;& \Phi_p(X) - T(p)X\Phi_p(X) + p^{k-1}X^2\Phi_p(X) \\ = \;& 1 + \big(T(p) - T(p)\big)X - \sum_{r\geq 2}\big(T(p^r) - T(p)T(p^{r-1}) + p^{k-1}T(p^{r-2})\big)X^r \end{aligned}$$

which is equal to 1 by theorem 27.

□

Definition 4.12. *The* **Dirichlet series** *of a sequence* $(a_n)_{n\in\mathbb{N}}$ *of complex numbers* a_n *is the series* $\sum_n a_n n^{-s}$.

The **Dirichlet series of a modular form** *is the Dirichlet series of its sequence of Fourier coefficients.*

Remark: By far the simplest[42] and most famous nontrivial example of a Dirichlet series is $\sum_n n^{-s}$ ie. the Dirichlet series of the of the constant sequence $a_n = 1$. This series is better known as the **Riemann Zeta function.**

Theorem 28. *The spinor L-function of* $f = \sum_{n\geq 1} a_n q^n$ *is equal to the Dirichlet series of* f.

Proof. A simple calculation using the explicit formula in corollary 4.2 confirms that that the system of Fourier coefficients of a cuspidal Hecke eigenform is multiplicative eg. $a_{nm} = a_n a_m$ whenever $\gcd(n, m) = 1$. The series defining the spinor L-series of f is known to be absolutely convergent for $\mathrm{Re}(s)$ sufficiently large [Borel, §14, theorem 14.2], and so we are permitted to rearrange the summation as we see fit. The particular way in which we see fit to do so is the following one:

$$\begin{aligned} L(f, \mathrm{spin}, s) &= \prod_p \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}} \\ &= \prod_p \Phi_p(p^{-s}) \\ &= \prod_p \sum_{r\geq 0} \frac{a_{p^r}}{p^{rs}} \\ &= \sum_{n\geq 1} \frac{a_n}{n^s} \end{aligned}$$

where on the last line we have invoked the fundamental theorem of arithmetic.

[42] For a given (and contestable!) value of "simple."

□

We shall now give an alternative statement of the modularity theorem 1 from §1. The reader would do well to compare the following statement to its earlier counterpart.

Theorem 29. (Taylor-Breuil-Conrad-Diamond) *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Then there exists a Hecke eigenform $f \in S_2\big((\Gamma_0(N_E)\big)$ with rational eigenvalues such that*

$$L(E,s) = L_{spin}(f,s).$$

5 Modularity

Philosophical Definition 5.1. *An abelian variety A over $\mathbb{Q}$ of dimension g is* **modular** *if there exists a modular form $F \in M_k(\Gamma)$ for some weight $k \in \mathbb{Z}$ and some arithmetic subgroup Γ of $Sp_{2g}(\mathbb{Q})$ together with a finite dimensional complex representation π of $GSpin_{2g+1}(\mathbb{C})$ such that*

$$L(A,s) = L(f,\pi,s)$$

.

The difficulties and deficiencies of this definition are several and glaring.

5.1 Partial L-series and "Automorphicity".

Insight from the theory of Galois representations enables us extend the definition of $L(A,s) = \prod_p L_p(A,s)$ over all primes p, including those p at which A has bad reduction. In contrast, given a general Hecke eigenform F of level $\Gamma \subsetneq \mathrm{Sp}_{2g}(\mathbb{Q})$ gor $g > 1$ and a finite dimensional complex representation $\pi : \mathrm{GSpin}_{2g+1}(\mathbb{C}) \to \mathrm{GL}(V)$ we have only succeeded in defining a partial L-series

$$\prod_{p \in S} L_p(f,\pi,s)$$

where S is the set of primes p for which the local Hecke algebra at p is unramified[43] If we wish to state a coherent analogue of the Taniyama-Shimira-Weil / Modularity Conjecture then it is incumbent upon us to show that there is a natural – and moreover *unique* – way to define $L_p(f,\pi,s)$ when $p \notin S$. It is a standard (but very much open) conjecture in the Langlands' program (see [Borel, especially §12]) that a suitable definition does indeed exist for partial L-series that are "*automorphic*" in origin.[44]

5.2 L-series versus L functions

Neither $L(A,s)$ nor $L(f,\pi,s)$ is known (outside of certain special cases) to have good analytic properties as a function an the complex plane. In particular, it has not been established that these L-series are actually **L-functions.**

[43] When $g = 1$ we can define the L-series of a Hecke eigenform f to be the Dirichlet series of f.

[44] We will not attempt to define what "automorphic" means in this context. Suffice it to say that this class of L-series encompasses (but vastly generalises) the L-series of Hecke eigenforms.

Philosophical Definition 5.2. *An* **L-function** *is a meromorphic function* $\phi : \mathbb{C} \to \mathbb{C}$ *with the following properties:*

(a) ϕ *is the meromorphic continuation of a function defined in some right half plane* $Re(s) > C$ $(C \in \mathbb{R} > 0)$ *by a Dirichlet series* $\sum_n a_n n^{-s}$*;*

(b) ϕ *has an* **Euler product***, ie. for* $Re(s) > C$ *one can write* $\phi(s)$ *as a product*

$$\phi(s) = \prod_p \phi_p(s)$$

of analytic functions ϕ_p *indexed by prime numbers* p*;*

(c) there exists a function ϕ_∞ *such that the function* $\Phi(s) := \phi_\infty(s)\phi(s)$ *is a meromorphic function on* $\mathbb{C}$ *with finitely many poles which moreover satisfies a functional equation relating its value at* s *to its value at* $\kappa - s$ *for some constant* $\kappa \in \mathbb{R}$ *(depending on* ϕ*).*

In full generality we have

Theorem 30. (Langlands), care of [Borel, §14 theorem 14.2].
For each Hecke eigenform F *and each finite dimensional complex representation* π *of* $GSpin_{2g+1}(\mathbb{C})$ *the partial* L *series*

$$\prod_{p \text{ unramified}} L_p(f, \pi, s)$$

is absolutely convergent in some right half plane.

For $g = 1$ and $g = 2$ we can do much better.

Theorem 31. *Let* N *be a positive integer and let* $f \in S_k\big(\Gamma_1(N)\big)$ *be a newform, ie. a cuspidal Hecke eigenform* $f(q) = \sum_{n \geq 1} a_n q^n$ *with* $a_1 = 1$ *such that* $f \notin M_k\big(\Gamma_1(M)\big)$ *for any proper divisor* M *of* N*. Let* $\Gamma(s) := \int_{t=0}^{\infty} t^{s-1} e^{-t} dt$ *be the familiar Gamma function from complex analysis. Then the function*

$$\Lambda(f, s) = N^{s/2} \frac{\Gamma(s)}{(2\pi)^s} L(f, s)$$

has an analytic continuation to an entire function on $\mathbb{C}$*. Moreover, there exists a second newform* $\tilde{f}$ *of the same weight and level as* f *and a constant* $W(f)$ *such that*

$$\Lambda(f, s) = W(f)\Lambda(\tilde{f}, k - s).$$

Theorem 32. *(***Andrianov)**
If $F \in M_k\big(Sp_4(\mathbb{Z})\big)$ *is a cuspidal Hecke eigenform then the function*

$$\Lambda_{spin}(F, s) := \Gamma(s)\Gamma(s - k + 2) L_{spin}(F, s)$$

is meromorphic on $\mathbb{C}$ *with finitely many poles and satisfies the functional equation*

$$\Lambda_{spin}(F, 2k - 2 - s) = (-1)\Lambda^k_{spin}(F, s).$$

For a full discussion and proof of these theorem, see [Rohrlich, section 3] (especially proposition 18 on page 85) and [A-Z] respectively.

5.3 Modularity of GL_2-type Abelian Varieties.

For a special class of abelian varieties a modularity theorem along the lines suggested by philosophical definition 5.1 is known due to work of Ribet and the proof of Serre's conjecture by Khare & Wintenberger.

Definition 5.1. *The* **endomorphism ring** *$End(A)$ of an abelian variety A is the ring of auto-isogenies of A under composition and pointwise addition. The* **rational endomorphism algebra** *of A is the $\mathbb{Q}$-algebra $End(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Definition 5.2. *An abelian variety A over $\mathbb{Q}$ is said to be of* **$\mathbf{GL}_2$-type** *if the rational endomorphism algebra $End(A) \otimes \mathbb{Q}$ is isomorphic to a number field of dimension $[End(A) \otimes \mathbb{Q} : \mathbb{Q}] = \dim A$ over $\mathbb{Q}$.*

In [Ribet, §4, theorem 4.4] it is shown that Serre's conjecture on the modularity of (odd) irreducible galois representations mod p implies that every abelian variety of GL_2-type is "classically modular."

5.4 Gritsenko Lifts and the Paramodular Conjecture

We conclude with a conjecture of Brumer & Kramer in [B-K] which – by virtue of being explicit enough to be computationally testable[45] – amounts to the current state-of-the-art modularity conjecture for $g = 2$.

Definition 5.3. *The* **paramodular group** *of level N is*

$$\Gamma[N] := \left\{ g \in Sp_4(\mathbb{Q}) \middle| g = \begin{pmatrix} * & * & N^{-1}* & * \\ N* & * & * & * \\ N* & N* & * & N* \\ N* & * & * & * \end{pmatrix} \right\},$$

where $*$ denotes an integer.

Remark: The paramodular group $\Gamma[N]$ can be shown to be conjugate (in $\mathrm{GL}_{2g}(\mathbb{Q})$) to the group $\mathrm{Sp}_(\mathrm{diag}(1, N), \mathbb{Z})$. Thus $\Gamma[N] \backslash \mathbb{H}^2$ is a (surrogate) coarse moduli space of polarized abelian surfaces with polarization of type $\mathrm{diag}(1, N)$.

For each positive integer N there exists, thanks to work of Skoruppa-Zaguier in [S-Z] and Gritsenko in [Gritsenko], an injective homomorphism from a certain subspace of the the space of elliptic cuspforms $S_k(\Gamma_0(N)$ to the space of **paramodular forms** $M_k(\Gamma[N])$. This homomorphism is known as the **Gritsenko lifting** and the paramodular forms in its image are known as **Gritsenko lifts** .

In [R-S] an analogue of the theory of Atkin-Lehner theory of old- and newforms on SL_2 is considered with respect to which the subspace of $M_k(\Gamma[N])$ consisting of Gritsenko lifts plays the role of "oldforms".[46] Brumer & Kramer define a **Gritsenko-non-lift** to be a cuspidal Hecke eigenform in the orthogonal complement of the space of Gritsenko lifts and advance the following precise conjecture.

Conjecture 5.1. (Brumer-Kramer 2010) Conjecture 1.1 in [B-K]
There is a one-to-one correspondence between isogeny classes of abelian surfaces A

[45] The paper [Poor-Yuen] details a continuing computational investigation of paramodular forms which has – thus far – borne out the conjecture of Brumer & Kramer.

[46] See §1 for the definitions of old- and newforms.

over $\mathbb{Q}$ of conductor N with $\mathrm{End}_{\mathbb{Q}}(A) = \mathbb{Z}$ and weight 2 non-lifts f *on the paramodular group $\Gamma[N]$ with rational eigenvalues, up to scalar multiplication. Moreover, the L-series $L(A, s)$ and $L_{spin}(f, s)$ should agree.*

6 References

[Andrianov] Anatoli Andrianov, *Introduction to Siegel Modular Forms and Dirichlet Series*, (Universitext). Springer-Verlag, New York, 2009.

[Artin] Michael Artin, "Néron Models." In Gary Cornell & Joseph H. Silverman (eds.), *Arithmetic Geometry.* Springer-Verlag, New York, 1986. DID I USE THIS?

[A-Z] Anatoli Andrianov & Vladimir Zhuravlev, *Modular forms and Hecke operators* (Translations of Mathematical Monographs volume 145). American Mathematical Society, 1995.

[B-K] Armand Brumer & Kenneth Kramer,"Paramodular Abelian Varieties of Odd Conductor." *Transactions of the American Mathematical Society,* Vol. 366 (2014), pp. 2463-2516.

[Borel] Armand Borel "Automorphic L-functions." In Armand Borel & William Casselman (eds.), *Proceedings of the Symposium in Pure Mathematics (part II), Volume XXXIII (Corvallis Oregon, 1997).* American Mathematical Society, Providence, 1979.

[Gritsenko] Valeri Gritsenko, "Arithmetical Lifting and its applications." In Sinnou david (ed.), *Number Thoery Paris 1992-3* (London Mathematical Society Lecture Note Series 215). Cambridge University Press, Cambridge, 1995.

[Hindry] Marc Hindry *Introduction to Zeta and L-functions from Arithmetic Geometry and some applications.* Notes from a mini-course at the University of Brasil's *XXI Escola de Álgebra,* July 2010. Notes freely available at the author's website:
`http://www.math.jussieu.fr/~hindry/actu_uk.html`

[Husemöller] Dale Husemöller, *Elliptic Curves (2nd edition)*, (Graduate Texts in Mathematics). Springer-Verlag, New York, 2004.

[Igusa] Jun-ichi Igusa, *Theta functions*, (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen Band 194). Springer-Verlag, Berlin, 1972.

[Klingen] Helmut Klingen, *Introductory Lectures on Siegel Modular Forms*, (Cambridge studies in advanced mathematics 20). Camrbridge University Press, 1990.

[Milne] J.S Milne, "Abelian Varieties." In Gary Cornell & Joseph H. Silverman (eds.), *Arithmetic Geometry.* Springer-Verlag, New York, 1986.

[Poor-Yuen] Cris Poor & David S. Yuen,"Paramodular Cusp Forms." To appear in *Mathematics of Computation.* arXiv:0912.0049.

[Ribet] Kenneth A. Ribet, "Abelian varieties over $\mathbb{Q}$ and modular forms." *Algebra and Topology 1992 (Taejon),*, Korea Adv. Inst. Sci. Tech. Taejon (1992), pp. 53-79.

[Rohrlich] David E. Rohrlich, "Modular Curves, Hecke Correspondences and L-functions." In Gary Cornell, Joseph H. Silverman & Glenn Stevens (eds.), *Modular Forms and Fermat's Last Theorem.* Springer-Verlag, New York, 1997.

[Rosen] Michael Rosen, "Abelian Varieties over $\mathbb{C}$." In Gary Cornell & Joseph H. Silverman (eds.), *Arithmetic Geometry*, Springer-Verlag, New York, 1986.

[R-S] Brooks Roberts and Ralf Schmidt, *Local Newforms for GSp_4*, (Lecture Notes in Mathematics 1918). Springer-Verlag, New York, 2007.

[Serre-Tate] Jean-Pierre Serre & John Tate, "Good Reduction of Abelian Varieties." *Annals of Mathematics*, Second Series, Vol. 88, No. 3 (Nov., 1968), pp. 492-517.

[Silverman] Joseph H. Silverman, "A Survery of the Arithmetic Theory of Elliptic Curves." In Gary Cornell, Joseph H. Silverman & Glenn Stevens (eds.), *Modular Forms and Fermat's Last Theorem.* Springer-Verlag, New York, 1997. DID I USE THIS?

[Springer] T.A. Springer, "Reductive Groups." In Armand Borel & William Casselman (eds.), *Proceedings of the Symposium in Pure Mathematics (part II), Volume XXXIII (Corvallis Oregon, 1997).* American Mathematical Society, Providence, 1979.

[Stevens] Glenn Stevens, "An Overview of the Proof of Fermat's Last Theorem." In Gary Cornell, Joseph H. Silverman & Glenn Stevens (eds.), *Modular Forms and Fermat's Last Theorem.* Springer-Verlag, New York, 1997.

[S-Z] Nils-Peter Skoruppa & Don Zagier,"Jacobi forms and a certain Space of modular forms." *Inventiones Mathematicae*, Vol. 94, (1988) pp. 113-146.

7 Appendix A. Galois representations

7.1 (Finite) Galois theory

Any ring homomorphism $\varphi : K \to L$ between fields K and L is necessarily injective and so induces **(i)** an isomorphism between K and a subfield $\varphi(K)$ of L and **(ii)** a K-algebra structure on L for which φ is the structure map. In this situation one says that L is an **extension** of K.[47]

Definition 7.1. *An extension L/K of fields is called* **finite** *if $[L : K] < \infty$, ie. if L is finite dimensional as an algebra over K.*

A powerful technique for studying the structure of an extension L/K is to consider the group $\mathrm{Aut}(L/K)$ of automorphisms of L as an element of the category Alg_K of K algebras.

According to taste, elements of $\mathrm{Aut}(L/K)$ can be thought of as ring homomorphisms $\sigma : L \to L$ such that $\sigma(x) = x$ for all $x \in K$, or else (should one wish to keep track of the particular extension mapping $K \to L$) as commuting diagrams

$$\begin{tikzcd}
L \arrow[rr, "\sigma"] & & L \\
& K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

It is an easy exercise to verify that for each subgroup H of $\mathrm{Aut}(L/K)$ the subset

$$L^H := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}$$

of L on which H acts trivially is in fact a sub*field* of L. We refer to L^H as the **fixed field** of H.

Definition 7.2. *An extension L/K of fields is called* **Galois** *if*

1. *L/K is finite;*

2. *$L^{Aut(L/K)} = K$, ie. no proper intermediate extension of K in L is fixed by every element of $Aut(L/K)$.*

When L/K is Galois we call $Aut(L/K)$ the **Galois group** *of the extension and denote it by $Gal(L/K)$.*

The power of this definition is made abundantly clear by the striking **fundamental theorem of Galois theory.**

Theorem 33. *If L/K is a Galois extension then*

1. *$[L : K] = \#Gal(L/K)$;*

2. *L/E is Galois for every subextension E/K contained in L;*

3. *subextensions of K in L are in one-to-one correspondence with subgroups of the Galois group, eg. if $K \subseteq E \subseteq L$ is a tower of extensions then $E = L^H$ for a unique subgroup H of $Gal(L/K)$;*

[47] One often writes "L/K is an extension" to indicate that L is an extension of K. It is – for better of worse – customary to suppress the homomorphism $\varphi : K \to L$ from the notation and to conflate K with its image $\varphi(K)$ in L.

4. *the extension L^H/K is Galois if and only H is a normal subgroup of Gal(L/K);*

5. *for each normal subgroup H of Gal(L/K) there is a canonical surjection Gal$(L/K) \to$ Gal(L^H/K) with kernel H.*

□

The surjective homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$ in the last part of the theorem is a simple restriction map eg. to each $\sigma \in \mathrm{Gal}(L/k)$ we associate the pullback of σ along the inclusion $H \hookrightarrow L$. That such a simple minded approach actually works follows from the part (4) of the theorem: to say that H is a normal subgroup of $\mathrm{Gal}(L/k)$ is to say that $\sigma H = H\sigma$ for all σ, in which case for all $x \in L^H$ we have

$$H\sigma x = \sigma H x = \sigma x.$$

and so $\sigma(L^H) = L^H$. That $\mathrm{Gal}(L/K)$ surjects onto $\mathrm{Gal}(L^H/K)$ is only slightly less trivial: one begins by choosing a basis $e_1, \dots, e_n$ for L over L^H with $e_1 = 1$ and then one defines for each K-linear automorphism $\psi : L^H \to L^H$ a lifting $\Psi : L \to L$ by letting ψ act diagonally with respect to the chosen basis, eg.

$$\Psi(\sum_{i=1}^n a_i e_i) := \sum_{i=1}^n \psi(a_i) e_i.$$

Clearly Ψ is K-linear, and one can easily check[48] that Ψ is multiplicative and thus a field automorphism of L.

7.2 Infinite Galois theory

Galois theoretical methods are sufficiently powerful, and the family of all Galois extensions of a given field K sufficiently orderly in structure, that one is able to take as one's objects of study not only Galois extensions of arbitrarily large degree but also arbitrarily large or even infinite *systems* of Galois extensions. Before we can hope to explain just what this last statement purports to mean we must first make a brief detour into abstract nonsense.

Let $\mathfrak{G}_K$ denote the subcategory of Alg_K whose objects are Galois extensions L/K and whose morphisms are K-linear field embeddings. Thus an object of $\mathfrak{G}_K$ is a diagram

$$\begin{tikzcd} L \\ K \arrow[u] \end{tikzcd}$$

with L/K Galois and an element of $\mathrm{Hom}_{\mathfrak{G}_K}(L, E)$ is a commuting diagram

$$\begin{tikzcd} L \arrow[rr, "f"] & & E \\ & K \arrow[ul] \arrow[ur] & \end{tikzcd}$$

[48] For example, by letting $\{x(i,j,k)\} \subseteq L^H$ be a set of structure constants satisfying $e_i e_j = \sum_k x(i,j,k) e_k$ for every i, j and hammering out the computation in coordinates.

where $f : L \to E$ is ring homomorphism.

Let L/K and E/K be any two Galois extensions. Fix an algebraic closure $K \to \overline{K}$ and let F be the subfield of $\overline{K}$ generated by the images of all embeddings (of which there $[L : K]$ and $[E : K]$ respectively) of L and E into $\overline{K}$. It turns out that F is a Galois extension of K in which both L and E are subextensions. The upshot is that for any two Galois extensions L, E of K there exists a third Galois extension F of K and a commuting diagram in $\mathfrak{G}_K$ of the form

$$\begin{tikzcd}
L \arrow[rr, bend left] & E \arrow[r] & F \\
& K \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

We have just shown that $\mathfrak{G}_K$ is an **inductive system**[49] in the category of K-algebras. By the fundamental theorem of Galois theory the corresponding family $\{\mathrm{Gal}(L/K)\}_{L\in\mathfrak{G}_K}$ of Galois groups forms a **projective system**[50] of finite groups in the category of groups. This projective system of Galois groups is the central object of study for "infinite Galois theory" and it is precisely this object that allows us to make sense of (and make good on) the grandiose claim made at the outset of this section.

7.3 The Absolute Galois Group

Definition 7.3. *Let K be a field. The* **absolute Galois group** G_K *of K is the projective limit in the category of groups of the projective system of all Galois groups for finite extensions of K. That is,*

$$G_K := \varprojlim_{L\in\mathfrak{G}_K} Gal(K/k).$$

More prosaically, an element $\sigma \in G_K$ is a family $\{\sigma_L \in \mathrm{Gal}(L/k)\}_{L\in\mathfrak{G}_K}$ such that whenever one has $L, E, F \in \mathfrak{G}_K$ with L a common subextension of E and F then the restriction to L of σ_E and σ_F agree. Alternatively, if one fixes an algebraic closure $K \to \overline{K}$ with compatible embeddings $\{L \to \overline{K}\}_{L\in\mathfrak{G}_K}$ then one may regard G_K as $\mathrm{Gal}(\overline{K}/K)$. We make mention of this only because the latter notation is extremely common in the literature.

Examples 7.1.

1. The algebraic closure of $\mathbb{R}$ is $\mathbb{C}$ and $[\mathbb{C} : \mathbb{R}] = 2$. Thus $G_{\mathbb{R}} \cong \mathbb{Z}/2\mathbb{Z}$ is the subgroup of $\mathrm{Aut}(\mathbb{C})$ generated by complex conjugation.

2. Let p be a prime number and let $K = \mathbb{F}_p$, the field of order p. Every finite extension of $\mathbb{F}_p$ is of the form $\mathbb{F}_{p^n}$ for some $n > 0$ and every such extension is

[49] An inductive (also known as **direct**) system is a (small) category $\mathcal{C}$ whose morphisms induce a partial order on the set of objects of $\mathcal{C}$ (ie. $x \le y$ if and only if there exists a morphism $x \to y$ in $\mathcal{C}$) with respect to which any two objects have a common lower bound.

[50] A projective (*aka* **inverse**) system is a (small) category $\mathcal{C}$ whose opposite category $\mathcal{C}^{\mathrm{op}}$ is an inductive system.

Galois. The Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic with canonical generator the **Frobenius automorphism**

$$\begin{array}{rcl} \mathrm{Frob}_p : \mathbb{F}_{p^n} & \to & \mathbb{F}_{p^n} \\ x & \mapsto & x^p \end{array}$$

and thus isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Passing to the projective limit we conclude that

$$G_{\mathbb{F}_p} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \;\cong\; \prod_{\text{prime } \ell} \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} \;=\; \prod_{\text{prime } \ell} \mathbb{Z}_\ell$$

where $\mathbb{Z}_\ell$ is the additive group of ℓ-adic integers.[51]

It is customary (not to mention advantageous) to endow G_k with a topology that reflects its construction as a projective limit of finite groups. The reader is gently reminded that G_K can be identified with a certain subset of the cartesian product of Galois groups corresponding to all Galois extensions of K.

Definition 7.4. *For each $L \in \mathfrak{G}_K$ endow Gal(L/K) with the discrete topology. The* **profinite topology** *on G_K is the topology induced by the inclusion*

$$G_K \hookrightarrow \prod_{L \in \mathfrak{G}_K} Gal(L/K)$$

where the ambient group is given the canonical product topology.[52]

We summarise the essential features of this topology.

- The topology of a topological group is uniquely determined by specifying an open neighbourhood base at its identity element. In G_K such a neighbourhood base is given by the set of all kernels of canonical projections $G_K \xrightarrow{\mathrm{proj}_L} \mathrm{Gal}(L/K)$ for $L \in \mathfrak{G}_K$. Since each group $\mathrm{Gal}(L/K)$ is finite, every such kernel subgroup is finite index. As a corollary, if $\mathcal{U}$ is any nonempty open subset of G_K then G_K is covered by finitely many translates of $\mathcal{U}$.
- By the fundamental theorem,

$$\ker\Big[G_k \to \mathrm{Gal}(L/k)\Big] = \Big(\prod_{E/L} \mathrm{Gal}(E/L) \prod_{F \in \mathfrak{G}_K, F \notin \mathfrak{G}_L} \mathrm{Gal}(F/K)\Big) \cap G_K.$$

  Thus the size of the open kernel of a projection map varies inversely with the degree of the corresponding extension. Suitably paraphrased, this says that "zooming in" at a point of G_K is tantamount to studying extensions of increasingly large degree over K.
- As $\mathrm{Gal}(L/K)$ is discrete for each L/K, each of the canonically open kernel subgroups is also *closed.*

[51] The group $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ is also known as the **profinite completion of the integers** and is often denoted by $\hat{\mathbb{Z}}$.

[52] Given a family $\{X_\lambda\}_\lambda$ of topological spaces, the product topology on $\prod_\lambda X_\lambda$ is the weakest topology in which every canonical projection $\prod_\lambda X_\lambda \xrightarrow{\mathrm{proj}_\lambda} X_\lambda$ is continuous.

- It is *not* the case that normal subgroups of G_K are in one-to-one correspondence with Galois extensions of K. Fortunately, the desired correspondence may be recovered by restricting one's attention to *closed* normal subgroups of G_K.

- Since any finite topological space is compact, Tychonoff's theorem implies that $\prod_{L\in\mathfrak{G}_K}\mathrm{Gal}(L/K)$ is compact. It is an elementary exercise in point set topology to show that G_K embeds into the product as a *closed* subgroup. Thus G_K is itself compact.

- G_K is **totally disconnected:** that is, a subset of G_K is connected if and only if it is a singleton set.

7.4 Number fields

In the case that K is a number field we can augment and rigidify G_K by exploiting the arithmetic of K to define useful auxiliary structures.

Definition 7.5. *A* **number field** *is a finite extension of the field of rational numbers* $\mathbb{Q}$*. If K is a number field then the* **ring of integers** *of K is the subring $\mathcal{O}_K$ of elements which are roots of monic integral polynomials:*

$$\mathcal{O}_K := \{x \in K \mid f(x) = 0 \, \textit{for some } f = a_nt^n + a_{n-1}t^{n-1} + \ldots + a_1t + a_0 \in \mathbb{Z}[t] \textit{ with } a_n = 1.\}$$

The ring $\mathcal{O}_K$ has fraction field K, is finitely generated as a module over $\mathbb{Z}$, and is an example of a **Dedekind domain**. Several equivalent definitions of the latter exist, the following being the most convenient for our purposes.

Definition 7.6. *A* **Dedekind domain** *is an integral domain $\mathcal{O}$ with the unique factorisation property at the level of ideals. That is, if $I \subseteq \mathcal{O}$ is a non-zero ideal then there exists a finite and unique collection of distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and unique positive integers $e_1, \ldots, e_n$ such that*

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}.$$

It follows immediately from the definition that in a Dedekind domain $\mathcal{O}$ every non-zero prime ideal is maximal.

Definition 7.7. *Let $\mathcal{O}$ be a Dedekind domain and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$. The* **residue field** *of $\mathcal{O}$ at $\mathfrak{p}$ is defined to be $\mathcal{O}/\mathfrak{p}$.*

In the case that $\mathcal{O} = \mathcal{O}_K$ for K a number field then the fact that $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module implies that every residue field is a *finite* field.

For the remainder of this document, whenever K is a number field we shall adopt the following notations (abusive and otherwise) and conventions:

- If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ then we will allow ourselves to call $\mathfrak{p}$ a prime of K.

- We will allow ourselves to refer to a residue field of $\mathcal{O}_K$ as a residue field of K.

- The residue field of K at $\mathfrak{p}$ will be denoted by $k_{\mathfrak{p}}$.

- We define $K_{\mathfrak{p}}$ to be the fraction field of the $\mathfrak{p}$-adic completion $\varprojlim_n \mathcal{O}_K/\mathfrak{p}^n$ of $\mathcal{O}_K$ at a prime ideal $\mathfrak{p}$. We will refer to this field as either the completion of K at $\mathfrak{p}$ or else the $\mathfrak{p}$-adic completion of K.

- The ring $\varprojlim_n \mathcal{O}_K/\mathfrak{p}^n$ itself will be denoted by $\mathcal{O}_{K_{\mathfrak{p}}}$ and referred to as either the ring of $\mathfrak{p}$-adic integers or else as the ring of integers of $K_{\mathfrak{p}}$.

It is clear that for any extension $\varphi : K \to L$ of number fields we have $\varphi(\mathcal{O}_K) \subseteq \mathcal{O}_L$.

Definition 7.8. *Let $K \to L$ be an extension of number fields and let $\mathfrak{p}$ be a prime of K. Let $\mathfrak{q}_1^{e1} \dots \mathfrak{q}_m^{em}$ be the unique factorisation of $\mathfrak{p}\mathcal{O}_L$ into distinct primes in L with multiplicities $e_1, \dots, e_m$. We say that $\mathfrak{p}$ is*

1. **split** *in L if $e_i = 1$ for all i;*
2. **ramified** *in L if $e_i > 1$ for some i;*
3. **inert** *in L if $\mathfrak{p}\mathcal{O}_L$ is prime.*

The primes $\mathfrak{q}_i$ appearing the factorisation are said to be primes **lying over** *(or simply* **over***) $\mathfrak{p}$. These are precisely the primes of $\mathcal{O}_L$ satisfying $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$. The multiplicities $e_1, \dots, e_n$ are variously called the* **ramification numbers** *or* **ramification degrees** *of $\mathfrak{p}$.*

When L/K is Galois it is a theorem that for each prime $\mathfrak{p}$ of $\mathcal{O}_K$ the action of $\text{Gal}(L/K)$ on L descends to a transitive permutation action on the set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_m\}$ of primes over $\mathfrak{p}$.

Definition 7.9. *Let L/K be a Galois extension of number fields and let $\mathfrak{q}$ be a prime over $\mathfrak{p}$. The* **decomposition group** *at $\mathfrak{q}$ is the stabiliser in Gal(L/K) of $\mathfrak{q}$ for its permutation action on primes over $\mathfrak{p}$:*

$$\mathfrak{D}_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in \mathit{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

It is clear from the definition that any two decomposition groups at primes over $\mathfrak{p}$ are conjugate in the Galois group.

The action of $\mathfrak{D}_{\mathfrak{q}/\mathfrak{p}}$ preserves $\mathfrak{q}$ and fixes $\mathfrak{p}$ pointwise and so descends to an automorphism of $l_{\mathfrak{q}} := L/\mathfrak{q}$ as an algebra over $k_{\mathfrak{p}} := K/\mathfrak{p}$. In other words, the decomposition group at $\mathfrak{q}$ is equipped with a natural homomorphism to the Galois group $\text{Gal}(l_{\mathfrak{q}}/k_{\mathfrak{p}})$ of the extension of (finite) residue fields.

Theorem 34. *Let L/K be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{q}$ be a prime of L over $\mathfrak{p}$. There is an isomorphism of groups*

$$\mathfrak{D}_{\mathfrak{q}/\mathfrak{p}} \xrightarrow{\sim} \mathit{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}).$$

Proof. Let $\nu : L_{\mathfrak{q}} \to \mathbb{Q} \cup \{\infty\}$ denote the $\mathfrak{q}$-adic discrete valuation and let $q \in \mathfrak{q}$ be a **uniformiser** for $L_{\mathfrak{q}}$[53] Then $\{x \in L_{\mathfrak{q}} \mid \nu(x) \geq 0\}$ is precisely the ring of integers $\mathcal{O}_{L_{\mathfrak{q}}}$ of $L_{\mathfrak{q}}$. We remark that every $\sigma \in \text{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ preserves both $\mathcal{O}_{L_{\mathfrak{q}}}$ and its maximal ideal

$$\mathfrak{q}\mathcal{O}_{L_{\mathfrak{q}}} = \{x \in L_{\mathfrak{q}} \mid \nu(x) > 0.\}$$

[53] A uniformiser in a discrete valuation ring is an element m of the unique maximal ideal $\mathfrak{m}$ with minimal $\mathfrak{m}$-adic valuation.

This is because **(i)** $\mathcal{O}_L$ is defined by a purely algebraic integrality condition and must therefore be preserved since $\mathbb{Q} \subseteq K_{\mathfrak{p}}$, and **(ii)** $\mathcal{O}_L$ embeds into its completion $\mathcal{O}_{L_{\mathfrak{q}}}$ as a dense subset. The maximal ideal $\mathfrak{q}\mathcal{O}_{\mathfrak{q}}$ is precisely the subset of $\mathcal{O}$ consisting of elements x such that the sequence $x, x^2, x^3, \ldots$ converges to zero in $\mathfrak{q}$-adic norm[54] and this set must necessarily be preserved by any (continuous) field automorhism of $L_{\mathfrak{q}}$.

As for the putative isomorphism, to each $\sigma \in \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ we may associate the restriction $\sigma|_L$ of σ to $L \subseteq L_{\mathfrak{q}}$, thus obtaining an automorphism of L fixing K pointwise and preserving $\mathfrak{q}$ ie. an element of $\mathfrak{D}_{\mathfrak{q}/\mathfrak{p}}$. This procedure of restriction is faithful since L is dense in $L_{\mathfrak{q}}$. Conversely, for each θ in the decomposition group at $\mathfrak{q}$ we obtain an automorphism $\theta_{\mathfrak{q}}$ of $L_{\mathfrak{q}}$ preserving both $\mathcal{O}_{\mathfrak{q}}$ and its maximal ideal (ie. a continuous automorphism) by defining

$$\theta_{\mathfrak{q}}(x) = \lim_{n\to\infty} \theta(x_n)$$

for any sequence $\{x_n\}$ in L converging to x.

□

In the course of the preceding proof it was shown that the action of $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ preserves both the ring of $\mathfrak{q}$-adic integers and its maximal ideal. Combining this observation with the conclusion of the theorem we see that there exists a natural homomorphism from the decomposition group $\mathfrak{D}_{\mathfrak{q}/\mathfrak{p}}$ to the Galois group of the extension of finite residue fields $l_{\mathfrak{q}}/k_{\mathfrak{p}}$.

Theorem 35. *For every prime $\mathfrak{p}$ of K and every prime $\mathfrak{q}$ of L over $\mathfrak{p}$ the natural homomorphism*

$$\mathfrak{D}_{\mathfrak{q}/\mathfrak{p}} \to Gal(l_{\mathfrak{q}}/k_{\mathfrak{p}})$$

is surjective.

Definition 7.10. *The* **inertia group** *at $\mathfrak{q}$, denoted $I_{\mathfrak{q}/\mathfrak{p}}$, is the kernel of the surjective homomorphism $\mathfrak{D}_{\mathfrak{q}/\mathfrak{p}} \to Gal(l_{\mathfrak{q}}/k_{\mathfrak{p}})$.*

To summarise: if L/K is a Galois extension of number fields then for each prime $\mathfrak{p}$ of K and each choice of prime $\mathfrak{q}$ over $\mathfrak{p}$ in of L (this choice being unique up to conjugation in $\mathrm{Gal}(L/K)$) we obtain a short exact sequence of groups of the form

$$1 \to I_{\mathfrak{q}/\mathfrak{p}} \to \mathfrak{D}_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(l_{\mathfrak{q}}/k_{\mathfrak{p}}) \to 1.$$

It can be shown that this sequence is well behaved under taking projective limits over all $L \in \mathfrak{G}_K$ (so long as one makes compatible choices of primes over $\mathfrak{p}$) in the sense that the sequence

$$1 \to \varprojlim_{L/K} I_{\mathfrak{q}/\mathfrak{p}} \to \varprojlim_{L/K} \mathfrak{D}_{\mathfrak{q}/\mathfrak{p}} \to \varprojlim_{L/K} \mathrm{Gal}(l_{\mathfrak{q}}/k_{\mathfrak{p}}) \to 1$$

is exact and the inverse limits of the decomposition and inertia groups corresponding to different compatible families of primes over $\mathfrak{p}$ are all conjugate in G_K. By abuse of notation, any subgroup of G_K conjugate to $\varprojlim_{L/K} \mathfrak{D}_{\mathfrak{q}/\mathfrak{p}}$ (resp. $\varprojlim_{L/K} I_{\mathfrak{q}/\mathfrak{p}}$) is referred to as *the* decomposition group $\mathfrak{D}_{\mathfrak{p}}$ (resp. *the* inertia group $I_{\mathfrak{p}}$) of G_K at $\mathfrak{p}$.

[54] The $\mathfrak{q}$-adic norm of x is $|l_{\mathfrak{q}}|^{-\nu(x)}$.

Remark: These short exact sequence can rewritten in the form

$$1 \to I_{\mathfrak{p}} \to G_{K_{\mathfrak{p}}} \to G_{k_{\mathfrak{p}}} \to 1.$$

While only cosmetically different, this new expression suggests a general strategy – or at the very least a philosophy – for attacking the Galois theory of number fields[55]: begin by studying the (far simpler and/or more controllable) Galois theory of their completions and their finite residue fields.

7.5 Galois representations

For general fields K the group G_K is far too complex to expect direct group theoretical methods (eg. group presentations) to be practicable, much less to bear fruit. This remains true even when one exploits to the fullest both topological methods and whatever auxilliary arithmetic data (such as that introduced in section 6.5) one might have to hand. One must suffer to study G_K indirectly, ie. by way of its actions and – in particular – of its continuous representation theory.

Definition 7.11. *A* **continuous representation** *of a topological group G on a vector space V is a continuous homomorphism $\rho : G \to GL(V)$.*

Remark: The continuity of a representation depends crucially on the choice of topology for $\mathrm{GL}(V)$. This in turn depends on the base field F of V. If $F = \mathbb{R}$ or $F = \mathbb{C}$ then $\mathrm{GL}(V)$ is to be understood as a Lie group. If F is a nonarchimedean local field (eg. $F = \mathbb{Q}_p$) then $GL(V)$ will be given the induced topology of its inclusion into F^{n^2} where $n = \dim V$. [56]. If F is a finite field then $\mathrm{GL}(V)$ will always be a discrete space. These stipulations ensure that whenever the vector space V is itself equipped with a natural topology then a representation $\rho : G \to \mathrm{GL}(V)$ is continuous (in the sense of the definition) if and only if for each $v_0 \in V$ the function

$$G \to V, \quad g \mapsto \rho(g)v_0$$

is continuous.

Henceforth all representations will be assumed continuous. A representation of an absolute Galois group G_K will be referred to as a **Galois representation.**

Definition 7.12. *Let K be a number field and let $\mathfrak{p}$ be a prime of K. A Galois representation $\rho : G_K \to GL(V)$ is said to be* **unramified** *at $\mathfrak{p}$ if $\rho(I_{\mathfrak{p}}) = 1$ for some (and hence every) inertia group at $\mathfrak{p}$. Otherwise, ρ is said to be* **ramified** *at $\mathfrak{p}$.*

One happy consequence of a Galois representation being unramified at $\mathfrak{p}$ is that for such representations and such primes we can transport useful structures backwards from the (well understood) absolute Galois groups of finite fields along the surjective homomorphisms $\mathfrak{D}_{\mathfrak{p}} \to G_{k_{\mathfrak{p}}}$. Recall that a Galois extension $K \to L$ of number fields induces Galois extensions $k_{\mathfrak{p}} \to l_{\mathfrak{q}}$ of finite residue fields for each prime

[55] And more generally, of **global fields**. In place of an honest definition we offer a complete classification: a global field is either **(i)** a number field or **(ii)** the field of rational functions on a projective algebraic curve over a finite field.

[56] In other words, $GL(V)$ will be a sort of "p-adic manifold." The technical name for such a thing is a **rigid analytic space**.

$\mathfrak{p}$ of K and each prime $\mathfrak{q}$ of L over $\mathfrak{p}$, and that if $|l_\mathfrak{q}| = |k_\mathfrak{p}|^n$ then $\mathrm{Gal}(l_\mathfrak{q}/k_\mathfrak{p})$ is a cyclic group of order n with canonical generator the **Frobenius automorphism** $x \mapsto x^n$. While it is no longer quite cyclic, the absolute Galois group $G_{k_\mathfrak{p}}$ nevertheless possesses a canonical *topological generator*[57]. This is an element $\phi_\mathfrak{p}$ of $G_{k_\mathfrak{p}}$ with the property that the image of $\phi_\mathfrak{p}$ in the Galois group of any finite extension of $k_\mathfrak{p}$ is the associated Frobenius automorphism. For technical reasons it is convenient to work not with $\phi_\mathfrak{p}$ itself but with its *inverse* $\mathrm{Frob}_\mathfrak{p} := \phi_\mathfrak{p}^{-1}$. [58]

Definition 7.13. *A* **Frobenius element** *of G_K is any inverse image of Frob$_\mathfrak{p}$ in any of the decomposition groups $\mathfrak{D}_\mathfrak{p}$ at $\mathfrak{p}$.*

From the short exact sequence

$$1 \to I_\mathfrak{p} \to \mathfrak{D}_\mathfrak{p} \to G_{k_\mathfrak{p}} \to 1$$

we see that the obstruction to pulling back the Frobenius element to a well defined element[59] of the decomposition group (and thus to an element of G_K itself) is precisely the existence of an inertia subgroup at $\mathfrak{p}$. The upshot is that – for all intents and purposes – this obstruction vanishes with respect to any Galois representation which is unramified at $\mathfrak{p}$.

The real power in the definition of a Frobenius element is revealed by the following striking corollary of **Chebotarev's density theorem:**

Theorem 36. *Let K be a number field. For each Galois representation $\rho : G_K \to GL(V)$ the set of (conjugacy classes) of Frobenius elements Frob$_\mathfrak{p}$ at primes of K where ρ is unramified generates a dense subgroup of G_K.*

Thus a Galois representation is uniquely determined by its values on Frobenius elements.

7.6 L-functions of Galois representations

Let K be a number field and let $\rho : G_K \to \mathrm{GL}(V)$ be a Galois representation on a finite dimensional vector space V. For each prime $\mathfrak{p}$ of K let $V^{I_\mathfrak{p}}$ denote the maximal subspace of V on which the inertia subgroup[60] at $\mathfrak{p}$ acts trivially:

$$V^{I_\mathfrak{p}} := \{v \in V \mid \rho(I^\mathfrak{p})v = v\}.$$

We remark that ρ may be restricted to a well defined representation $\mathfrak{D}_\mathfrak{p} \to \mathrm{GL}(V^{I_\mathfrak{p}})$: indeed, $I_\mathfrak{p}$ is a normal subgroup[61] of $\mathfrak{D}_\mathfrak{p}$ and so $\rho(I_\mathfrak{p})\rho(\sigma)v = \rho(\sigma)\rho(I_\mathfrak{p})v = \rho(\sigma)v$ for all $\sigma \in \mathfrak{D}\mathfrak{p}$ and all $v \in V^{I_\mathfrak{p}}$.

Before giving the central definition of this section, we briefly recall that the **norm** $N\mathfrak{p}$ of an ideal $\mathfrak{p}$ in a number field K is the cardinality of its residue field, ie. $N\mathfrak{p} := |k_\mathfrak{p}|$.

[57] A **topological generator** in a topological group G is an element which generates a dense subgroup.

[58] In the context of Étale cohomology (where the distinction becomes important) one refers to Frob$_\mathfrak{p}$ as the **geometric** Frobenius and to $\phi_\mathfrak{p}$ as the **arithmetic** Frobenius.

[59] Technically a conjugacy class of elements, but this will turn out to be sufficiently well defined for our purposes.

[60] This definition does not depend on the choice of $I_\mathfrak{p}$ in its conjugacy class.

[61] Recall that the inertia subgroup at $\mathfrak{p}$ is defined as the kernel of a homomorphism out of the corresponding decomposition group.

Definition 7.14. *The* **L-function** *of a Galois representation $\rho : G_K \to GL(V)$ is the function of a complex variable s defined by the infinite product*

$$L(\rho, s) := \prod_{\mathfrak{p}} \det(I - N\mathfrak{p}^{-s}\rho(\mathit{Frob}_{\mathfrak{p}})|V^{I_{\mathfrak{p}}})^{-1}$$

where

$$\det(I - X\rho(\mathit{Frob}_{\mathfrak{p}})|V^{I_{\mathfrak{p}}})$$

is the characteristic polynomial (in a variable X) of $\mathit{Frob}_{\mathfrak{p}}$ acting on $V^{I_{\mathfrak{p}}}$. $L(\rho, s)$ is to be understood as being defined for s in the largest possible right half plane in $\mathbb{C}$ for which the infinite product makes sense and converges absolutely.

8 Appendix B. Line bundles on projective spaces.

In this brief section we present the classification of line bundles of projective space. These line bundles are (strictly peaking) not examples of the line bundles discussed in the preceding section since we will need to quotient by a group action with continuous orbits. Nevertheless, the line bundles in question can be presented in a virtually identical way.

For each $k \in \mathbb{Z}$ and $n \in \mathbb{N}$ we have the following action of $\mathbb{C}^\times$ on $\mathbb{C}^{n+1}\backslash\{0\} \times \mathbb{C}$:

$$\alpha\big((z_0, \dots, z_n), p\big) := \big(\alpha z_0, \dots, \alpha z_n), \alpha^k p\big).$$

Let $\mathbb{C}^\times\backslash_k\mathbb{C}^{n+1}\backslash\{0\}\times\mathbb{C}$ denote the orbit space of this action and write $[(z_0, \dots, z_n), p]$ for the image of $\big((z_0, \dots, z_n), p\big)$ under the quotient mapping.

Definition 8.1. *The line bundle $\mathcal{O}(k)$ is the bundle on $\mathbb{P}^n$ with total space $\mathbb{C}^\times\backslash_k\mathbb{C}^{n+1}\backslash\{0\}\times\mathbb{C}$ and bundle map*

$$\begin{array}{rcl} \pi_k : \mathbb{C}^times\backslash_k\mathbb{C}^{n+1}\backslash\{0\} \times \mathbb{C} & \to & \mathbb{P}^n, \\ [(z_0, \dots, z_n), p] & \mapsto & [z_0 : \dots : z_n]. \end{array}$$

A global section s of $\mathcal{O}(k)$ can be identified with a function $f : \mathbb{C}^{n+1}\backslash\{0\}\times\mathbb{C} \to \mathbb{C}$ via

$$s([z_0 : \dots : z_n]) = [(z_0, \dots, z_n), f(z_0, \dots, z_n)]$$

and if s is to be well defined it must satisfy

$$\begin{aligned} [(\alpha z_0, \dots, \alpha z_n), \alpha^k f(z_0, \dots, z_n)] &= [(z_0, \dots, z_n), f(z_0, \dots, z_n)] = s([z_0 : \dots : z_n]) \\ &= s([\alpha z_0 : \dots : \alpha z_n]) \\ &= [(\alpha z_0, \dots, \alpha z_n), f(\alpha z_0, \dots, \alpha z_n)]. \end{aligned}$$

In other words, f must be a homogeneous polynomial of degree k. Conversely, it is easy to see that every homogeneous polynomial of degree k is a global section of $\mathcal{O}(-k)$. We have shown

Lemma 8.1. *Let $I_k = \{\underline{i} = (i_0, \dots, i_n) \in \mathbb{Z}_{\geq 0}^{n+1} \mid \sum_j i_j = k\}$. Then*

$$H^0\big(\mathbb{P}^n, \mathcal{O}(-k)\big) = \mathbb{C}[t_0, \dots, t_n]_k := \bigoplus_{\underline{i} \in I_k} \mathbb{C}t_0^{i_0}t_1^{i_1}\dots t_n^{i_n}.$$

Remark: It is trivial to see that $\mathcal{O}(k) \otimes_{\mathbb{C}} \mathcal{O}_m \cong \mathcal{O}(k+m)$ and that $\mathcal{O}(0)$ is a trivial line bundle.

The line bundles $\mathcal{O}(-1)$ and $\mathcal{O}(1)$ are singled out for special attention since their tensor products generate the whole family $\{\mathcal{O}(k) \mid k \in \mathbb{Z}\}$.

Definition 8.2. *The* **tautological line bundle** *on* $\mathbb{P}^n$ *is* $\mathcal{O}(-1)$.
The **hyperplane line bundle** *on* P^n *is* $\mathcal{O}(1)$.

The tautological bundle is so named because it is isomorphic to the meromorphic line bundle encoding the transition functions for the "standard" affine open charts $\{(\mathcal{U}_i, \varphi_i) \mid 0 \le i \le n\}$ of $\mathbb{P}_n$ where

$$\begin{array}{rcl} \mathcal{U}_i := \{[z_0 : \ldots : z_n] \in \mathbb{P}^n \mid z_i \neq 0\} & \xrightarrow{\varphi_i} & \mathbb{C}^i \times \{1\} \times \mathbb{C}^{n-1}, \\ {[z_0 : \ldots, z_{i-1} : z_i : z_{i+1} : \ldots : z_n]} & \mapsto & (z_0/z_i, \ldots, z_{i-1}/z_i, 1, z_{i+1}/z_i, \ldots, z_n/z_i). \end{array}$$

with transition function τ_{ji} over $\mathcal{U}_i \cap \mathcal{U}_j$ given by coordinate-wise multiplication by z_i/z_j, eg.

$$\begin{array}{rcl} \tau_{ji}\varphi_i\big([z_0 : \ldots : z_n]\big) & = & \tau_{ij}\big(\frac{z_0}{z_i}, \ldots, \frac{z_i}{z_i}, \ldots, \frac{z_j}{z_i}, \ldots, \frac{z_n}{z_i}\big) \\ & := & \frac{z_i}{z_j}\big(\frac{z_0}{z_i}, \ldots, \frac{z_i}{z_i}, \ldots, \frac{z_j}{z_i}, \ldots, \frac{z_n}{z_i}\big) \\ & = & \big(\frac{z_0}{z_j}, \ldots, \frac{z_i}{z_j}, \ldots, \frac{z_j}{z_j}, \ldots, \frac{z_n}{z_j}\big) \\ & = & \varphi_j\big([z_0 : \ldots : z_n]\big). \end{array}$$

A meromorphic global section s of this "transition function" bundle can be identified with a meromorphic function $f : \mathbb{C}^n \to \mathbb{C}$ via its restrictions

$$s|_{\mathcal{U}_i}([z_0 : \ldots : z_n]) = \big(\frac{z_0}{z_i}, \ldots, \frac{z_n}{z_i}, f(z_1/z_i, \ldots, z_n/z_i)\big)$$

and the compatibility of s with the transtition functions τ_{ji} implies that $\tau_{ji} f \varphi_i = f \circ \varphi_j$ ie.

$$\frac{z_i}{z_j} f(z_1/z_j, \ldots, z_n/z_j)) = f(z_1/z_i, , \ldots, z_n/z_i) = f\big(\frac{z_j}{z_i} z_1/z_j, \ldots, \frac{z_j}{z_i} z_n/z_j\big)$$

and so f must be homogeneous of degree -1. It is now routine to verify that the transition function bundle for $\mathbb{P}^n$ is isormophic to $\mathcal{O}(-1)$ as claimed.

The hyperplane bundle $\mathcal{O}(1)$ is so named because the divisor (=zero locus in $\mathbb{P}^n$) of any non-zero section s of $\mathcal{O}(1)$ is the flat hyperplane cut out by the corresponding homogenous function $f_s \in \mathbb{C}[t_0, \ldots, t_n]_1$.

Theorem 37. *Every meromorphic line bundle on* $\mathbb{P}^n$ *is isomorphic to* $\mathcal{O}(k)$ *for some* $k \in \mathbb{Z}$.

9 Appendix C. Group Cohomology

If G is a group and A is a G-module then we form a chain complex

$$C^0(G, A) \xrightarrow{d^0} C^1(G, A) \xrightarrow{d^1} C^2(G, A) \xrightarrow{d^2} \ldots$$

where the group $C^n(G,A)$ of n-**cochains** is the set of all functions $\phi : G^n \to A$ under pointwise addition and where the differential $d^n : C^n(G,A) \to C^{n+1}(G,A)$ is defined on n-cochains f by the formula

$$\begin{aligned} d^n f(g_1,\ldots,g_{n+1}) &= gf(g_2,\ldots,g_{n+1}) \\ &\quad +\sum_{i=1}^{n}(-1)^i f(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_n) \\ &\quad +(-1)^{n+1}f(g_1,\ldots,g_n). \end{aligned}$$

The n^{th} **cohomology of** G **with coefficients in** A is by definition

$$\mathrm{H}^n(G,A) = \frac{\ker(d^n)}{\mathrm{im}(d^{n-1})}.$$

Remark: The set $C^0(G,A)$ of 0-cochains is precisely[62] the underlying abelian group of A. For each $a \in A = C^0(G,A)$, $d^0a \in C^1(G,A)$ is the function $g \mapsto d^0a(g) := ga - a$. To say that $a \in \ker(d^0)$ is thus to say that $ga = a$ for all $g \in G$ and since $H^0(G,A) = \ker(d^0)$ it follows that $H^0(G,A) = A^G$ is the **group of invariants** of A under G. Indeed, $H^n(G,A)$ turns out to be the n^{th} (left) derived functor of the functor

$$(*)^G : G\text{-Mod} \to \mathbb{Z}\text{-Mod}, \qquad A \mapsto A^G$$

taking G-modules to their groups of G-invariant elements.

[62] According to taste, this is either a tautology (ie. one simply defines $C^0(G,A)$ this way) or else a consequence of categorical nonsense. Notice first of all that G^0 cannot be the empty set since we are working in the category of groups. Secondly, the n-fold cartesian product G^n is defined by a universal mapping property: for each group M there is a natural isomorphism $\mathrm{Hom}(M,G^n) \xrightarrow{\sim} \Big(\mathrm{Hom}(M,G)\Big)^n$, or in other words one obtains a unique homomorphism $M \to G^n$ whenever one chooses exactly n homomorphisms $M \to G$. When $n = 0$ this says that one obtains a canonical homomorphism $M \to G^0$ whenever one chooses no homomorphisms at all from M to G, ie. G^0 should be a group for which there exists a canonical homorphism $M \to G^0$ for each group M. Then G^0 is a terminal object in the category of groups, which is to say that G^0 is a trivial group. Clambering back up and out from our own navels we conclude that functions $G^0 \to A$ are in bijection with A.