BUNTES

BU Number Theory Expository Seminar

BUNTES

BU Number Theory Expository Seminar

BUNTES Attendees (notes by Alex)

November 19, 2018

Contents

Chapter 1

Abelian Varieties

These are notes for BUNTES Fall 2017, the topic is Abelian varieties, they were last updated November 19, 2018. We are using Milne's abelian varieties notes primarily, for more details see the webpage. These notes are by Alex, feel free to email me at `alex.j.best@gmail.com` to report typos/suggest improvements, I'll be forever grateful.

1.1 Introduction (Angus)

1.1.1 Definitions

Definition 1.1.1 Abelian varieties. An **abelian variety** is a complete connected algebraic group. ◊

Definition 1.1.2 Algebraic groups. An **algebraic group** is an algebraic variety G along with regular maps $m\colon G\times G \to G$, $e\colon * \to G$, $\mathrm{inv}\colon G \to G$ such that the following diagrams commute.
Identity

$$\begin{tikzcd} * \times G \arrow[r, "e\times\mathrm{id}"] \arrow[dr, "\sim"'] & G\times G \arrow[d, "m"] & G\times * \arrow[l, "\mathrm{id}\times e"'] \arrow[dl, "\sim"] \\ & G & \end{tikzcd}$$

Inverse

$$\begin{tikzcd} G \arrow[r, "\mathrm{inv},\mathrm{id}"] \arrow[d] & G\times G \arrow[d, "m"] & G \arrow[l, "\mathrm{id},\mathrm{inv}"'] \arrow[d] \\ * \arrow[r, "e"'] & G & * \arrow[l, "e"'] \end{tikzcd}$$

Associativity

$$\begin{tikzcd} G\times G\times G \arrow[r, "\mathrm{id}\times m"] \arrow[d, "m\times\mathrm{id}"'] & G\times G \arrow[d, "m"] \\ G\times G \arrow[r, "m"'] & G \end{tikzcd}$$

◊

Definition 1.1.3 Complete varieties. A variety X is **complete** if every projection map

$$X \times Y \to Y$$

is closed. ◊

Example 1.1.4 Abelian varieties.

- Elliptic curves.
- Weil restriction $\mathrm{Res}_{K/\mathbf{Q}} E$ of an elliptic curve E.
- Jacobian varieties of curves.

□

Plan:

- Some motivation via elliptic curves.
- Gathering some material about "completeness".
- Prove that abelian varieties are abelian.

1.1.2 Elliptic curves (char(k) $\neq 2, 3$)

Theorem 1.1.5 *TFAE for a projective curve E over k.*

1. *E is given by $Y^2Z = X^3 + aXZ^2 + bZ^3$, $4a^3 + 27b^2 \neq 0$.*
2. *E is nonsingular of genus 1 with a distinguished point P_0.*
3. *E is nonsingular with an algebraic group structure.*
4. *(if $k \subseteq \mathbf{C}$) such that $E(\mathbf{C}) = \mathbf{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbf{C}$.*

Proof. Strategy: Item 1 $\iff$ Item 2 $\iff$ Item 3 and Item 2 $\implies$ Item 4 $\implies$ Item 1.

Item 1 $\implies$ Item 2 is done.

Item 2 $\implies$ Item 1: Riemann-Roch states that $l(D) = l(K-D)+\deg(D)+1-g$ so here $l(D) = l(K-D) + \deg(D)$ further is $D > 0$ then $l(K-D) = 0$ in which case $l(D) = \deg(D)$. Consider $L(nP_0)$ for $n > 0$ Riemann-Roch implies that $l(nP_0) = n$ then it always contains the constants.

$$L(P_0) = k$$

$$L(2P_0) = k \oplus kx$$

$$L(3P_0) = k \oplus kx \oplus ky$$

$$\vdots$$

$$L(6P_0) = k \oplus kx \oplus ky \oplus kx^2 \oplus ky^2 \oplus kxy \oplus kx^3/\sim$$

so we must have a relation which after manipulation is of the desired form. We get an embedding

$$E \hookrightarrow \mathbf{P}^2$$

$$P \mapsto (x(P) : y(P) : 1)\,(P \neq P_0)$$

$$P_0 \mapsto (0 : 1 : 0)$$

and thus E is of the desired form. ■

Definition 1.1.6 Elliptic curves. An **elliptic curve** over k is any/all of that 1.1.5. $\lozenge$

Which of the above characterisations generalise to abelian varieties?

1. No, in general we don't know that the equations look like.
2. One could possibly replace "genus" with a condition on the dimension of cohomology groups.
3. Yes, this is essentially the definition.
4. Yes, stay tuned!

1.1.3 Complete varieties

Idea: if $X \times Y$ had product topology (instead of its Zariski topology) then complete is equivalent to compact.

We'd like to gather a few results about complete varieties we can use to access properties of abelian varieties (like abelianness).

Proposition 1.1.7 *Let V be a complete variety. Given any morphism $\phi\colon V \to W$ $\phi(V)$ is closed.*

Proof. Let $\Gamma_\phi = \{(v, \phi(v))\} \subseteq V \times W$ be the graph of ϕ. Its a closed subvariety of $V \times W$. Under the projection $V \times W \to W$, the image of Γ_ϕ is $\phi(V)$ and thus closed. ■

Corollary 1.1.8 *If V is complete and connected, any regular function on V is constant.*

Proof. A regular function is a morphism $f\colon V \to \mathbf{A}^1$. By the above $f(V) \subseteq \mathbf{A}^1$ is closed, and this is a finite set of points. But connected implies we just have one point. ■

Corollary 1.1.9 *Let V be a complete connected variety. Let W be an affine variety. Given $\phi\colon V \to W$, then $\phi(V)$ is a point.*

Proof. We have an embedding $W \hookrightarrow \mathbf{A}^n$. On $\mathbf{A}^n$ we have the coordinate functions $\mathbf{A}^n \xrightarrow{x_i} \mathbf{A}^1$. The composition

$$V \xrightarrow{\phi} W \hookrightarrow \mathbf{A}^n \to \mathbf{A}^1$$

be the above is constant. Thus the coordinates of $\phi(V)$ are constant, so $\phi(V) = \{\mathrm{pt}\}$. ■

A final result of interest that I won't prove today:

Theorem 1.1.10 *Projective varieties are complete.*

The main goal of this section is to prove the following theorem:

Theorem 1.1.11 Rigidity. *Let V, W be varieties such that V is complete and $V \times W$ is geometrically irreducible. Let $\alpha\colon V \times W \to U$ be a morphism such that $\exists u_0 \in U(k), v_0 \in V(k), w_0 \in W(k)$ with $\alpha(V \times \{w_0\}) = \alpha(\{v_0\} \times W) = \{u_0\}$. Then $\alpha(V \times W) = \{u_0\}$.*

Proof. Since $V \times W$ is geometrically irreducible, V must be connected. Denote the projection $q\colon V \times W \to W$. Let $U_0 \ni u_0$ be an open neighborhood. We consider the set

$$Z = \{w \in W : \alpha((v, w)) \notin U_0 \text{ for some } v \in V\} = q(\alpha^{-1}(U \smallsetminus U_0))$$

Since q is closed, $Z \subseteq W$ is closed. Since $w_0 \in W \smallsetminus Z$, $W \smallsetminus Z$ is a nonempty open subset of W.

Consider $w \in W \smallsetminus Z$. Since $V \times \{w\} \cong V$ it is complete and connected. Thus

$$\alpha(V \times \{w\}) = \{\mathrm{pt}\} = \alpha((v_0, w)) = \{u_0\}$$

which implies that

$$\alpha(V \times (W \smallsetminus Z)) = \{u_0\}$$

Since $V \times (W \smallsetminus Z) \subseteq V \times W$ is open and $V \times W$ is irreducible, it is dense. So $\alpha(V \times W) = \{u_0\}$. ∎

Proposition 1.1.12 *Let A, B be abelian varieties. Every morphism $\alpha\colon A \to B$ is the composition of a homomorphism and a translation.*

Proof. First compose by a translation on B such that $\alpha(0) = 0$. Consider the map

$$\begin{aligned}\phi\colon A \times A &\to B\\ (a, a') &\mapsto \alpha(a + a') - \alpha(A) - \alpha(a')\end{aligned}$$

Then

$$\begin{aligned}\phi(A \times \{0\}) &= \alpha(a + 0) - \alpha(a) - \alpha(0) = 0\\ \phi(\{0\} \times A) &= \alpha(0 + a) - \alpha(0) - \alpha(a) = 0.\end{aligned}$$

By the rigidity theorem 1.1.11 $\phi(A \times A) = \{0\}$ hence $\alpha(a + a') = \alpha(a) + \alpha(a')$. ∎

Corollary 1.1.13 *Abelian varieties are abelian.*

Proof. The inversion map $a \mapsto -a$ sends 0 to 0, thus is a homomorphism. Therefore

$$a + b - a - b = a + b - (a + b) = 0$$

and so

$$a + b = b + a.$$ ∎

1.2 Abelian varieties over C (Alex)

The goal of this talk is to understand what abelian varieties look like over $\mathbf{C}$. The goal for me is to understand what a (principal) polarisation is and why it is important.

First immediate question: why study complex theory at all? The most classical field, algebraically closed, archimidean, characteristic 0.

Recall/rapidly learn the picture for elliptic curves, given E an elliptic curve we have for some Λ a rank 2 lattice in $\mathbf{C}$

$$\begin{aligned}\mathbf{C}/\Lambda &\xrightarrow{\sim} E(\mathbf{C}) \subseteq \mathbf{P}^2(\mathbf{C})\\ z &\mapsto (\wp(z) : \wp'(z) : 1)\\ 0 &\mapsto (0 : 1 : 0)\end{aligned}$$

where
$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}.$$
This is a meromorphic function whose image lands in
$$y^2 = 4x^3 - g_2 x - g_3.$$
So the $\mathbf{C}$ points of an elliptic curve are topologically a torus.

1.2.1 Abelian varieties

Naturally one asks: does this generalise? Let A be an abelian variety over $\mathbf{C}$, what does $A(\mathbf{C})$ look like? Another torus?

Proposition 1.2.1 *$A(\mathbf{C})$ is a compact, connected, complex lie group.*

Proposition 1.2.2 *Let A be an abelian variety of dimension g over $\mathbf{C}$. Then we have*
$$A(\mathbf{C}) \cong V/\Lambda$$
where V is a g dimensional complex vector space and Λ is a full rank lattice of V (i.e Λ is a discrete subgroup of V s.t. $\mathbf{R} \otimes \Lambda = V$).

Proof. Differential geometry gives us a map of complex manifolds, the exponential map
$$\exp\colon \operatorname{Tgt}_0(A(\mathbf{C})) \to A(\mathbf{C})$$
this is holomorphic. And since $A(\mathbf{C})$ is abelian, this is a homomorphism also. In general this is locally an isomorphism around 0.

Claim: exp is injective. There exists a neighborhood $U \supseteq 0$ s.t. $\exp(U) \cong U$. Consider the image $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$. For $x \in \exp(\operatorname{Tgt}_0 A(\mathbf{C}))$, $\{U + x\}$ are all open and give a cover. Thus $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$ is open. Since $A(\mathbf{C})$ is connected we are thus reduced to showing $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$ is closed also. Since exp is a homomorphism, the image is a subgroup. So its complement is the union of its non-trivial cosets, which is open. Thus $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$ is closed. Giving $\exp(\operatorname{Tgt}_0 A(\mathbf{C})) = A(\mathbf{C})$, which proves the claim.

exp is a local isomorphism, which gives that ker(exp) is discrete, i.e. a lattice. We now have
$$A(\mathbf{C}) \cong \operatorname{Tgt}_0 A(\mathbf{C})/\ker(\exp)$$
so as $A(\mathbf{C})$ is compact we cannot have a kernel which is not full rank, as otherwise the quotient could not be compact. ■

Definition 1.2.3 We call any such V/Λ a **complex torus**. ◊

From the above isomorphism we can now read off properties of $A(\mathbf{C})$ as a group.

Proposition 1.2.4 *$A(\mathbf{C})$ is divisible, and $A(\mathbf{C})[n] \cong (\mathbf{Z}/n\mathbf{Z})^{2g}$.*

Proof.
$$A(\mathbf{C}) \cong V/\Lambda \cong (\mathbf{R}/\mathbf{Z})^{2g}$$
isomorphisms as groups, thus $A(\mathbf{C})$ is divisible. Further, $(\mathbf{R}/\mathbf{Z})[n] = (\frac{1}{n}\mathbf{Z})/\mathbf{Z}$. ■

Question: Given a complex torus V/Λ, does there exist an abelian variety A such that $A(\mathbf{C}) \cong V/\Lambda$?

Example 1.2.5

- $$\mathbf{C}/\Lambda \cong E(\mathbf{C}) \text{ always in dim 1}$$
- $$\mathbf{C}^2/\Lambda^2 \cong (E \times E)(\mathbf{C}) \text{ sometimes yes in higher dimension}$$
- $$\mathbf{C}^2/\langle (i,0),(i\sqrt{p},i),(1,0),(0,1)\rangle_{\mathbf{Z}}$$
  for p prime??? (I guess not, see Mumford)

□

Theorem 1.2.6 Chow. *If X is an analytic submanifold of $\mathbf{P}^n(\mathbf{C})$ then X is an algebraic subvariety.*

By this theorem it is enough to analytically imbed $V/\Lambda \hookrightarrow \mathbf{P}^m$. We can try and do this by mimicing the elliptic curve strategy, find enough functions $\theta\colon V/\Lambda \to \mathbf{C}$.

1.2.2 Cohomology

Proposition 1.2.7 *Let $X = V/\Lambda$. Then*

$$H^r(X,\mathbf{Z}) \cong \{\textit{alternating } r\textit{-forms } \Lambda \times \cdots \times \Lambda \to \mathbf{Z}\}.$$

Proof. $\pi\colon V \to V/\Lambda$ is a universal covering map, so

$$\Lambda = \pi^{-1}(0) \cong \pi_1(X,0).$$

Because all these spaces are nice

$$H^1(X,\mathbf{Z}) \cong \mathrm{Hom}(\pi_1(X),\mathbf{Z}) \cong \mathrm{Hom}(\Lambda,\mathbf{Z}).$$

To extend to $r \neq 1$ use the Künneth formula:

$$\begin{tikzcd}
\bigwedge^r(H^1(X_1\times X_2,\mathbf{Z})) \arrow[r, equal] \arrow[d, equal, "\text{Künneth}"] & H^r(X_1\times X_2,\mathbf{Z}) \arrow[dd, equal, "\text{Künneth}"] \\
\bigwedge^r(H^1(X_1,\mathbf{Z})\otimes H^1(X_2,\mathbf{Z})) \arrow[d, equal] & \\
\bigoplus_{p+q=r}(\bigwedge^p(H^1(X_1,\mathbf{Z}))\otimes \bigwedge^q(H^1(X_2,\mathbf{Z}))) \arrow[r, equal] & \bigoplus_{p+q=r}(H^p(X_1,\mathbf{Z})\otimes H^q(X_2,\mathbf{Z}))
\end{tikzcd}$$

Since we know the proposition for $S^1 = \mathbf{R}/\mathbf{Z}$ by taking products and applying the above we get it for all complex tori V/Λ. ■

Proposition 1.2.8 *There is a correspondence*

$$\{\textit{Hermitian forms } H \textit{ on } V\} \leftrightarrow \{\textit{Alternating forms } E\colon V\times V \to \mathbf{R},\ E(iu,iv) = E(u,v)\}$$
$$H \mapsto \operatorname{im} H$$
$$E(iu,v) + iE(u,v) \leftarrow E.$$

1.2.3 Line bundles

Now we will consider line bundles on $X = V/\Lambda$, that is

$$L \xrightarrow{\pi} X$$

such that for any $x \in X$ there exists $U \ni x$ with $\pi^{-1}(U) \cong \mathbf{C} \times U$. We can obtain these from hermitian forms and some auxilliary data as follows.

Definition 1.2.9 If H is a hermitian form on V such that $E(\Lambda \times \Lambda) \subseteq \mathbf{Z}$ there exists a map

$$\alpha\colon \Lambda \to \mathbf{C}^* = \{z \in \mathbf{C}^* : |z| = 1\}$$

such that

$$\alpha(u + v) = e^{i\pi E(u,v)}\alpha(u)\alpha(v).$$

Further, there is a line bundle $L(H, \alpha)$ on X which is defined by quotienting $\mathbf{C} \times V$ by Λ which acts via

$$\phi_u(\lambda, v) = (\alpha(u)e^{\pi H(v,u)+\frac{1}{2}\pi H(u,u)}\lambda, v + u) \text{ for } u \in \Lambda,$$

we'll denote by e_u the factor $\alpha(u)e^{\pi H(v,u)+\frac{1}{2}\pi H(u,u)}$ for brevity. ◊

Theorem 1.2.10 Appell-Humbert. *Any line bundle on X is of the form $L(H, \alpha)$ for some H, α as above. Further*

$$L(H_1, \alpha_1) \otimes L(H_2, \alpha_2) = L(H_1 + H_2, \alpha_1\alpha_2).$$

In fact we have the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}(\Lambda, \mathbf{C}) \arrow[r] \arrow[d] & \{\textit{data } (H, \alpha)\} \arrow[r] \arrow[d] & \{\textit{gp. of Herm. } H \textit{ w/ } E(\Lambda \times \Lambda) \subseteq \mathbf{Z}\} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Pic}^0(X) \arrow[r] & \mathrm{Pic}(X) \arrow[r, "c"'] & \ker(H^2(X, \mathbf{Z}) \to H^2(X, \mathcal{O}_X)) \arrow[r] & 0
\end{tikzcd}$$

where $\mathrm{Pic}(X)$ is the group of all line bundles on X and Pic^0 is the subgroup of those which are topologically trivial.

We wanted functions $X \to \mathbf{C}$. Now we can instead consider sections s of $L(H, \alpha) \xrightarrow{\pi} X$ i.e. maps $s\colon X \to L(H, \alpha)$ with $\pi \circ s = \mathrm{id}$. Denote the space of such sections $H^0(X, L(H, \alpha))$.

Definition 1.2.11 Theta functions. The sections of $L(H, \alpha)$ correspond to holomorphic functions

$$\theta\colon V \to \mathbf{C}$$

such that $\theta(z + u) = e_u\theta(z)$, we will call such a θ a **theta function** for (H, α).◊

If H is not positive definite the space of such functions is 0!

Proposition 1.2.12 *If H is positive definite, then the dimension of $H^0(X, L(H, \alpha))$ is $\sqrt{\det E}$ where we really mean the determinant of a matrix for E with respect to an integral basis.*

Theorem 1.2.13 Lefschetz. *Given a positive definite H, there exists an imbedding $X \hookrightarrow \mathbf{P}^m$.*

Proof. Sketch: Let $L = L(H, \alpha)$, consider $L(H, \alpha)^{\otimes 3} = L(3H, \alpha^3)$, take a basis of $\theta_0, \dots, \theta_d$ of $H^0(X, L^{\otimes 3})$.

Claim: $\Theta \colon z \mapsto (\theta_0(z) : \cdots : \theta_d(z)) \subseteq \mathbf{P}^d$ is an embedding.

To see that this is well defined, we must give a section of $L^{\otimes 3}$ not vanishing at z for all $z \in X$. Let $\theta \in H^0(X, L) \setminus \{0\}$. Then pick a, b such that the section of $L^{\otimes 3}$ given by

$$\theta(z-a)\theta(z-b)\theta(z+a+b)$$

does not vanish. This is possible and thus we have a nonvanishing section of $L^{\otimes 3}$.

For injectivity, show that if the above section has the same values on z_1, z_2 then it is a theta function for some sublattice. Almost all sections aren't theta functions for a sublattice (this uses Proposition 1.2.12).

Something similar must be done for tangent vectors. ■

Definition 1.2.14 Riemann forms. A **Riemann form** is $E \colon \Lambda \times \Lambda \to \mathbf{Z}$ alternating such that

$$E_{\mathbf{R}} \colon V \times V \to \mathbf{R}$$

has the property that $E(iu, iv) = E(u, v)$ and the corresponding Hermitian form is positive definite. ◊

Definition 1.2.15 Polarizable tori. A complex torus $X = V/\Lambda$ is **polarizable** if there exists a Riemann form E on Λ. ◊

Example 1.2.16 Proposition. Every $\mathbf{C}/\Lambda$ where $\Lambda = \langle 1, \tau \rangle_{\mathbf{Z}}$ is polarizable. To see this take

$$E(u, v) = \frac{u\bar{v}}{\operatorname{im} \tau}$$

as a Riemann form. □

Putting everything together we have obtained an equivalence of categories

$$\{\text{abelian varieties over } \mathbf{C}\} \leftrightarrow \{\text{polarizable complex tori}\}.$$

1.2.4 Isogenies

Definition 1.2.17 Isogenies of complex tori. An **isogeny** of complex tori is a homomorphism $V/\Lambda \to V'/\Lambda'$ with finite kernel. ◊

Definition 1.2.18 Dual vector spaces. Given V a complex vector space, let

$$V^* = \{f \colon V \to \mathbf{C} : f(u+v) = f(u) + f(v),\ f(\alpha v) = \bar{\alpha} f(v)\}$$

and given $\Lambda \subset V$ a lattice, let

$$\Lambda^* = \{f \in V^* : f(\lambda) \in \mathbf{Z}\, \forall \lambda \in \Lambda\}.$$

◊

Definition 1.2.19 Dual tori. If $X = V/\Lambda$, $X^\vee = V^*/\Lambda^*$ is the **dual torus**. ◊

Proposition 1.2.20 Existence of Weil pairing.

$$X \times X^\vee \to \mathbf{C}$$

so

$$X[n] \times X^\vee[n] \to \left(\frac{1}{n^2}\mathbf{Z}/\frac{1}{n}\mathbf{Z}\right) \cong \mathbf{Z}/n\mathbf{Z}$$

this is called the ***Weil pairing****.*

Can a complex torus be isogenous to its own dual? If X is polarizable then

$$\begin{aligned} X &\to X^\vee \\ v &\mapsto H(v, -) \end{aligned}$$

is an isogeny.

Definition 1.2.21 A **polarization** is an isogeny $X \to X^\vee$. ◊

1.3 Rational Maps into Abelian Varieties (Maria)

Note all varieties are irreducible today.

1.3.1 Rational maps

V, W varieties $/K$. Consider pairs (U, ϕ_U), where $\emptyset \neq U \subset V$ an open subset so U is dense, and $\phi_U : U \to W$ is a regular map.

Definition 1.3.1 Rational maps. (U, ϕ_U), $(U', \phi_{U'})$ are equivalent if ϕ_U and $\phi_{U'}$ agree on $U \cap U'$. An equivalence class ϕ of $\{(U, \phi_U)\}$ is a **rational map** $\phi: V \dashrightarrow W$ If $\phi: V \dashrightarrow W$ is defined at $v \in V$ if $v \in U$ for some $(U, \phi_U) \in \phi$. ◊

Note 1.3.2 The set $U_1 = \bigcup U$ where ϕ is defined is open and $(U_1, \phi_1) \in \phi$ where $\phi_1 : U_1 \to W$ restricts to ϕ_U on U.

Example 1.3.3

1. Let $\emptyset \neq W \subseteq V$ be open. Then the rational map $V \dashrightarrow W$ induced by $\mathrm{id}: W \to W$ will not extend to V. To avoid this, assume W is complete (so $W = V$).

2. $C: y^2 = x^3$, then $\alpha: \mathbf{A}^1 \to C, a \mapsto (a^2, a^3)$ is a regular map, restricting to an isomorphism $\mathbf{A}^1 \smallsetminus \{0\} \to C \smallsetminus \{0\}$. The inverse of $\alpha|_{\mathbf{A}^1 \smallsetminus \{0\}}$ represents $\beta: C \dashrightarrow \mathbf{A}^1$ which does not extend to C. This corresponds on function fields to
$$K(t) \to K(x, y)$$
$$t \mapsto y/x$$
which does not send $K[y]_{(t)}$ to $K[x, y]_{(x,y)}$.

3. Given a nonsingular surface V, $P \in V$ then $\exists \alpha: W \to V$ regular that induces an isomorphism $\alpha: W \smallsetminus \alpha^{-1}(P) \to V \smallsetminus P$, but $\alpha^{-1}(P)$ is a projective line. The rational map represented by α^{-1} is not regular on V (where to send P?).

□

Theorem 1.3.4 Milne 3.1. *A rational map $\phi: V \dashrightarrow W$ from a nonsingular variety V to a complete variety W is defined on an open subset $U \subseteq V$ whose complement has codimension ≥ 2.*

Proof. (V a curve) V nonsingular curve, $\emptyset \neq U \subseteq V$ open, $\phi\colon U \to W$ a regular map.

$$\begin{tikzcd}
 & V \\
U \arrow[ur] \arrow[r] \arrow[dr] & U' \subseteq Z \subseteq V \times W \ni (v,w) \arrow[u, "p"'] \arrow[d, "q"] \\
 & W \ni w
\end{tikzcd}$$

U' is the image of U, $Z = \overline{U'}$. W is complete, Z closed implies $p(Z) \subseteq V$ is closed. Also, $U \subseteq p(Z) \implies p(Z) = V$.

$$U \xrightarrow{\sim} U' \to U$$

so

$$U' \xrightarrow{\sim} U$$

$$Z \twoheadrightarrow V$$

this implies $Z \xrightarrow{\sim} V$. Then $q|_Z\colon Z \to W$ is the extension of ϕ to V. ■

Theorem 1.3.5 Milne 3.2. *A rational map $\phi\colon V \dashrightarrow A$ from a nonsingular variety V to an abelian variety W, extends to all of V.*

Proof. Theorem 1.3.4 Lemma 1.3.6 ■

Lemma 1.3.6 *Let $\phi\colon V \dashrightarrow G$ be a map from a nonsingular variety to a group variety. Then either ϕ is defined on all of V or the set where ϕ is not defined is closed of pure codimension 1.*

Proof. Fix $(U, \phi_U) \in \phi$ and consider

$$\Phi\colon V \times V \dashrightarrow G$$

represented by

$$U \times U \xrightarrow{\phi_U \times \phi_U} G \times G \xrightarrow{\mathrm{id} \times \mathrm{inv}} G \times G \xrightarrow{m} G$$

$$(x, y) \mapsto \phi_U(x)\phi_U(y)^{-1}$$

Check ϕ is defined at x iff Φ is defined at (x, x) (and in this case $\Phi(x, x) = e$). This is equivalent to the map $\Phi^*\colon \mathcal{O}_{G,e} \to K(V \times V)$ induced by Φ satisfying $\mathrm{im}(\mathcal{O}_{G,e}) \subseteq \mathcal{O}_{V \times V,(x,x)}$ For a nonzero function f on $V \times V$, write $\mathrm{div}(f) = \mathrm{div}(f)_0 - \mathrm{div}(f)_\infty$ which are effective divisors. Then

$$\mathcal{O}_{V \times V,(x,x)} = \{0\} \cup \{f \in K(V \times V) : \mathrm{div}(f)_\infty \text{ does not contain } (x, x)\}.$$

Suppose ϕ is not defined at x, then there exists $f \in \mathrm{im}(\mathcal{O}_{G,e})$ s.t. $(x, x) \in \mathrm{div}(f)_\infty$. Then Φ is not defined at any $(y, y) \in \Delta \cap \mathrm{div}(f)_\infty = \mathrm{div}(f^{-1})_0$, which is a pure codimension 1 subset of Δ by Milne's AG thm 9.2. The corresponding subset in V is of pure codimension 1, and ϕ is not defined there. ■

Theorem 1.3.7 Milne 3.4. *Let $\alpha\colon V \times W \to A$ be a morphism from a product of nonsingular varieties into an abelian variety. If $\alpha(V \times \{w_0\}) = \{a_0\} = \alpha(\{v_0\} \times W)$ for some $a_0 \in A$, $v_0 \in W$, $w_0 \in W$, then $\alpha(V \times W) = \{a_0\}$.*

Corollary 1.3.8 Milne 3.7. *Every rational map $\alpha\colon G \dashrightarrow A$ from a group variety into an abelian variety is the composition of a homomorphism and a translation in A.*

Proof. Since group varieties are nonsingular, $\alpha\colon G \to A$ is a regular map by Theorem 1.3.5. The rest is as proof of Corollary 1.2. ∎

1.3.2 Dominating and birational maps

Definition 1.3.9 Dominating maps. $\phi\colon V \dashrightarrow W$ is **dominating** if $\operatorname{im}(\phi_U)$ is dense in W for a representative $(U, \phi_U) \in \phi$. ◊

Exercise: A dominating $\phi\colon V \dashrightarrow W$ defines a homomorphism $K(W) \to K(V)$ and any such homomorphism arises from a unique dominating rational map.

Definition 1.3.10 $\phi\colon V \dashrightarrow W$ is **birational** if the corresponding $K(W) \to K(V)$ is an isomorphism or, equivalently if there exists $\psi\colon W \dashrightarrow V$ s.t. $\phi \circ \psi$ and $\psi \circ \phi$ are the identity wherever they are defined. In this case we say V and W are **birationally equivalent**. ◊

Note 1.3.11 In general birational equivalence does not imply isomorphic. E.g. V a variety $\emptyset \neq W \subsetneq V$ an open subset, or $V = \mathbf{A}^1, W\colon y^2 = x^3$.

Theorem 1.3.12 Milne 3.8. *If two abelian varieties are birationally equivalent then they are isomorphic as abelian varieties.*

Proof. A, B abelian varieties with $\phi\colon A \dashrightarrow B$ a birational map with inverse ψ. Then by Theorem 1.3.5 ϕ, ψ extend to regular maps $\phi\colon A \to B$, $\psi\colon B \to A$ and $\phi \circ \psi, \psi \circ \phi$ are the identity everywhere. This implies that ϕ is an isomorphism of algebraic varieties and after composition with a translation, ϕ is also a group isomorphism. ∎

Proposition 1.3.13 Milne 3.9. *Any rational map $\mathbf{A}^1 \dashrightarrow A$ or $\mathbf{P}^1 \dashrightarrow A$, for A an abelian variety is constant.*

Proof. Theorem 1.3.5 implies $\alpha\colon \mathbf{A}^1 \dashrightarrow A$ extends to $\alpha\colon \mathbf{A}^1 \to A$ and we may assume $\alpha(0) = e$. $(\mathbf{A}^1, +)$: $\alpha(x + y) = \alpha(x) + \alpha(y)$ for all $x, y \in \mathbf{A}^1(K) = K$. $(\mathbf{A}^1 \setminus \{0\}, \cdot)$: $\alpha(xy) = \alpha(x) + \alpha(y) + c$ for all $x, y \in K^\times$. These can only hold at the same time if α is constant. $\mathbf{P}^1 \dashrightarrow A$ is constant, since its constant on affine patches. ∎

Definition 1.3.14 $V/\overline{K}$ is **unirational** if there is a dominating map $\mathbf{A}^n \dashrightarrow V$, where $n = \dim_{\overline{K}} V$. V/K is unirational if V/K is. ◊

Proposition 1.3.15 Milne 3.10. *Every rational map $V \dashrightarrow A$ from V unirational to A abelian is constant.*

Proof. Wlog $K = \overline{K}$. Since V is unirational we get $\beta\colon \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \dashrightarrow V \dashrightarrow A$, which extends to $\beta\colon \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \to A$. Then by Milne corollary 1.5, there exist regular maps $\beta_i\colon \mathbf{P}^1 \to A$ s.t. $\beta(x_1, \ldots, x_n) = \sum \beta_i(x_i)$ and by Proposition 1.3.13 each β_i map is constant. ∎

1.4 Theorem of the Cube (Ricky)

1.4.1 Crash Course in Line Bundles

Consider $\mathbf{R}^2$, $f: \mathbf{R} \to \mathbf{R}$, $f(x, y) = x^2 + y^2 - 1$, now $S = \{f = 0\} \subseteq \mathbf{R}^2$ is a closed submanifold (in fact a circle). Question: Do all closed submanifolds arise in this way? Lets switch to $\mathbf{C}$ better analogies with AG.

Example 1.4.1 Let $X \in \mathbf{P}^n(\mathbf{C})$, the answer here is no! (Because $f: X \to \mathbf{C}^1$ is constant!) Want to define functions locally that give us level sets, but gluing such will give us a global section. Instead glue in a different way (i.e. into different "copies" of $\mathbf{C}$) so that this doesn't happen. □

Example 1.4.2 $X \in \mathbf{P}^1_{\mathbf{C}}$, $\mathcal{O}_X$ the structure sheaf.

$$X = U_0 \cup U_1 = (\mathbf{A}^1, t) \cup (\mathbf{A}^1, s)$$

on $U_0 \cap U_1$, $t = s^{-1}$. What is a global section of $\mathcal{O}_X$, a section of U_0 and a section of U_1 that glue. $\mathcal{O}_X(U_0) = k[t], \mathcal{O}_X(U_1) = k[s]$ so given $f(t), g(s)$ these glue to a global section iff $f(t) = g(1/t)$ so f, g must be constant. □

Definition 1.4.3 Line bundles. A **line bundle** on X is a locally free $\mathcal{O}_X$-module of rank 1, i.e. $\exists \{U_i\}$ open cover along with isomorphisms $\phi_i : \mathcal{L}|_{U_i} \xrightarrow{\sim} \mathcal{O}_X|_{U_i}$. ◊

Exercise 1.4.4 Alternative definition: A line bundle on X is equivalent to the following data:

- An open cover of X.
- Transition maps $\tau_{ij} \in \mathrm{GL}_1(\mathcal{O}_X(U_i \cap U_j))$ satisfying $\tau_{ij}\tau_{jk} = \tau_{ik}$ and $\tau_{ii} = \mathrm{id}$.

Example 1.4.5 On $X = \mathbf{P}^n_k$, we have line bundles $\mathcal{O}(d)$ for all $d \in \mathbf{Z}$. Just have to give cover and transition functions, use usual open cover $\{U_i\}$ with $U_i \cong \mathbf{A}^n$. Then τ_{ji} is given by multiplication by $(x_i/x_j)^d$. □

Exercise 1.4.6

$$H^0(X, \mathcal{O}(d))(= \Gamma(X, \mathcal{O}(d)))$$

$= k$vector space spanned by deg. d homogenous polynomials in $k[x_0, \ldots, x_n]$.

Exercise 1.4.7 All line bundles on $\mathbf{P}^n$ are isomorphic to some $\mathcal{O}(d)$.

We say a line bundle $\mathcal{L}$ on X is trivial if $\mathcal{L} \cong \mathcal{O}_X$. Given $\mathcal{L}_1$ and $\mathcal{L}_2$ on X (line bundles) we can create a new line bundle $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$. So isomorphism classes of line bundles on X with $\otimes$ form a group, denoted $\mathrm{Pic}(X)$ with identity $\mathcal{O}_X$ and inverses $\mathcal{L}^{-1} = \mathrm{Hom}(\mathcal{L}, \mathcal{O}_X)$.

Example 1.4.8 By previous exercise $\mathrm{Pic}(\mathbf{P}^n_k) \cong \mathbf{Z}$ since $\mathcal{O}_X(d_1) \otimes \mathcal{O}_X(d_2) \cong \mathcal{O}_X(d_1 + d_2)$. □

Fact 1.4.9 *If $f: X \to Y$, then given $\mathcal{L}$ on Y we can pullback to a line bundle $f^*\mathcal{L}$ on X, definition is complicated. We also know that f^* commutes with $\otimes$ so in fact (as $f^*\mathcal{O}_Y = \mathcal{O}_X$) we get a homomorphism $f^*: \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$.*

1.4.2 Relation to (Weil) divisors

Let X be a normal variety, call $Z \subsetneq X$, a closed subvariety of codimension 1, a **prime divisor**. Then a divisor on X is a formal sum

$$D = \sum_{Z \subsetneq X} n_Z \cdot Z$$

of prime divisors.

Let $K = K(X)$ be the function field of X. Given $f \in K^\times$ we can define

$$\operatorname{div}(f) = \sum v_Z(f) \cdot Z.$$

Given $D \in \operatorname{Div}(X)$, we can define a line bundle $\mathcal{L}(D)$ on X via

$$\mathcal{L}(D)(U) = \{f \in K^\times : (D + \operatorname{div}(f))|_U \geq 0\} \cup \{0\}$$

where $D|_U = \sum_{Z \cap U \neq \emptyset} n_Z \cdot (Z \cap U)$.

Proposition 1.4.10 *The map*

$$\operatorname{Cl}(X) = \operatorname{Div}(X)/\operatorname{Princ}(X) \xrightarrow{\mathcal{L}(\cdot)} \operatorname{Pic}(X)$$

is an isomorphism.

1.4.3 Onto cubes

Theorem 1.4.11 Theorem of the cube. *Let U, V, W be complete varieties. If $\mathcal{L}$ is a line bundle on $U \times V \times W$ s.t. $\mathcal{L}|_{\{u_0\}\times V \times W}, \mathcal{L}|_{U \times \{v_0\} \times W}, \mathcal{L}|_{U \times V \times \{w_0\}}$ are all trivial then $\mathcal{L}$ is trivial.*

Corollary 1.4.12 Milne 5.2. *Let A be an abelian variety. Let $p_i : A \times A \times A \to A$ be the projection onto the ith coordinate. $p_{ij} = p_i + p_j$, $p_{123} = p_1 + p_2 + p_3$. Then for any $\mathcal{L}$ on A, the line bundle*

$$\mathcal{M} = p_{123}^* \mathcal{L} \otimes p_{12}^* \mathcal{L}^{-1} \otimes p_{23}^* \mathcal{L}^{-1} \otimes p_{13}^* \mathcal{L}^{-1} \otimes p_1^* \mathcal{L} \otimes p_2^* \mathcal{L} \otimes p_3^* \mathcal{L}$$

is trivial.

Proof. Let $m : A \times A \to A$ be multiplication (addition?) and p, q the projections $A \times A \to A$. Then the composites of the maps $\phi : A \times A \to A \times A \times A$, $\phi(x, y) = (x, y, 0)$ with $p_{123}, p_{12}, p_{23}, p_{13}, p_1, p_2, p_3$ are respectively $m, m, q, p, p, q, 0$. Hence the restriction of $\mathcal{M}$ to $A \times A \times \{0\}$ is

$$m^* \mathcal{L} \otimes m^* \mathcal{L}^{-1} \otimes q^* \mathcal{L}^{-1} \otimes p^* \mathcal{L}^{-1} \otimes p^* \mathcal{L} \otimes q^* \mathcal{L} \otimes \mathcal{O}_{A \times A}$$

this is trivial by tensor commuting with pullback. Similarly $\mathcal{M}$ restricts to a trivial bundle on $A \times \{0\} \times A$ and $\{0\} \times A \times A$. So by theorem of the cube 1.4.11 $\mathcal{M}$ is trivial. ∎

Corollary 1.4.13 Milne 5.3. *Let $f, g, h : V \to A$ (A abelian). Then for any $\mathcal{L}$ on A the bundle*

$$\mathcal{M} = (f+g+h)^* \mathcal{L} \otimes (f+g)^* \mathcal{L}^{-1} \otimes (f+h)^* \mathcal{L}^{-1} \otimes (g+h)^* \mathcal{L}^{-1} \otimes f^* \mathcal{L} \otimes g^* \mathcal{L} \otimes h^* \mathcal{L}$$

is trivial.

Proof. $\mathcal{M}$ is the pullback of the line bundle of Corollary 1.4.12 via the map $(f,g,h)\colon V \to A \times A \times A$. ∎

On A we have $n_A\colon A \to A$ be $n_A(a) = a + \cdots + a$ (n times) for $n \in \mathbf{Z}$.

Corollary 1.4.14 Milne 5.4. *For $\mathcal{L}$ on A we have*

$$n_A^* \mathcal{L} \cong \mathcal{L}^{(n^2+n)/2} \otimes (-1)_A^* \mathcal{L}^{(n^2-n)/2}$$

In particular if $(-1)^* \mathcal{L} = \mathcal{L}$ (symmetric) then $n_A^* \mathcal{L} = \mathcal{L}^{n^2}$. And if $(-1)^* \mathcal{L} = \mathcal{L}^{-1}$ (antisymmetric) then $n_A^* \mathcal{L} = \mathcal{L}^n$.

Proof. Use Corollary 1.4.13 with $f = n_A, g = 1_A, h = (-1)_A$. So the line bundle

$$(n)^* \mathcal{L} \otimes (n+1)^* \mathcal{L}^{-1} \otimes (n-1)^* \mathcal{L}^{-1} \otimes (1-1)^* \mathcal{L}^{-1} \otimes n^* \mathcal{L} \otimes 1^* \mathcal{L} \otimes (-1)^* \mathcal{L}$$

is trivial i.e.

$$(n+1)^* \mathcal{L} = (n-1)^* \mathcal{L}^{-1} \otimes n^* \mathcal{L}^2 \otimes \mathcal{L} \otimes (-1)^* \mathcal{L}$$

in statement $n = 1$ is clear, so use $n = 1$ in the above to get

$$2_A^* \mathcal{L} \cong \mathcal{L}^2 \otimes \mathcal{L} \otimes (-1)_A^* \mathcal{L} \cong \mathcal{L}^3 \otimes (-1)_A^* \mathcal{L}.$$

Then induct on n in above. ∎

Theorem 1.4.15 Theorem of the square (Milne 5.5). *Let $\mathcal{L}$ be an invertible sheaf (line bundle) on A. Let $t_a\colon A \to A$ be translation by $a \in A(k)$. Then*

$$t_{a+b}^* \mathcal{L} \otimes \mathcal{L} \cong t_a^* \mathcal{L} \otimes t_b^* \mathcal{L}.$$

Proof. Use Corollary 1.4.13 with $f = \mathrm{id}$, $g(x) = a, h(x) = b$ to get

$$t_{a+b}^* \mathcal{L} \otimes t_a^* \mathcal{L}^{-1} \otimes t_b^* \mathcal{L}^{-1} \otimes \mathcal{L}$$

is trivial. ∎

Remark 1.4.16 Tensor by $\mathcal{L}^{-2}$ in the above equation to get

$$t_{a+b}^* \mathcal{L} \otimes \mathcal{L}^{-1} \cong (t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}) \otimes (t_b^* \mathcal{L} \otimes \mathcal{L}^{-1}).$$

This gives a group homomorphism

$$A(k) \to \mathrm{Pic}(A)$$

via

$$a \mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

for any $\mathcal{L} \in \mathrm{Pic}(A)$.

1.5 The Adventures of BUNTES (Sachi)

1.5.1 In which we are introduced to an important homomorphism, review some concepts and our story begins

Abelian variety X, we know this is a complete group variety, our goal is to give an embedding $X \to \mathbf{P}^N$ for some N. This motivates the study of line bundles.

Last time Ricky proved theorem of cube 1.4.11 and square 1.4.15. For any line bundle L on X, there is a group homomorphism $\Phi_L\colon X \to \mathrm{Pic}(X)$ via $x \mapsto T_x^* L \otimes L^{-1}$. Be careful T_x^* is $-x$, convention, who knows why.

Example 1.5.1 Let $X = E$ an elliptic curve, $L = L((0))$, $x \mapsto (x) - (0)$, in this case this is in $\mathrm{Pic}^0(E) \cong E \cong \widehat{E}$, □

Proposition 1.5.2 *This is translation invariant.*

Proof. Translate by $q \in E$. $(x+q) - (q)$ take p to be the third point on the line with x, q, $(x) + (q) + (p) \cong 3(0)$ and $(x+q) + (p) \cong 2(0)$ subtracting these gives $(x) - (x+q) + (q) \cong (0)$ or $(x) - (0) \cong (x+q) - (q)$. ■

What about the converse of this, what can we say about translation invariant line bundles

$$K(L) = \{x \in X : T_x^* L \cong L\}?$$

Proposition 1.5.3 *$K(L)$ is Zariski closed in X.*

Proof. Consider $m^* L \otimes p_2^* L^{-1}$ on $X \times X$, then

$$\{x : \text{this is trivial on } \{x\} \times X\}$$

is closed. See-saw 1.6.6 implies restriction is pullback

$$T_x^* L \otimes L^{-1}$$

so this is $K(L)$. ■

1.5.2 In which Pooh discovers our main theorem

Proposition 1.5.4 *Let X be an abelian variety and L a line bundle, $L = L(D)$ then TFAE:*

1. *$H(D) = \{x \in X : T_x^* D = D\}$ is finite.*
2. *$K(L) = \{x \in X : T_x^* L \cong L\}$ is finite.*
3. *$|2D|$ is basepoint free and defines a finite morphism $X \to \mathbf{P}^N$.*
4. *L is ample.*

Proof. *3. to 4.*. Is algebraic geometry.

2. to 1.. Follows as being equal is stronger than being linearly equivalent.

4. to 2.. Section 1.5.3

3. to 4.. Section 1.5.4 ■

1.5.3 In which Owl proves the ampleness of L implies finiteness of $K(L)$

4. to 2. Assume L ample and $K(L)$ is infinite. Let Y be the connected component at 0 of $K(L)$, $\dim Y > 0$. Show trivial bundle is ample on Y implies Y is affine, But Y is closed and therefore complete so this is a contradiction. $L|_Y$ ample $[-1]^* L|_Y$ is ample. $L|_Y \otimes [-1]^* L|_Y$ is ample, consider

$$\begin{aligned} d\colon Y &\to Y \times Y \\ y &\mapsto (y, -y) \end{aligned}$$

$m \circ d = \text{constant}$, $d^* m^*(L) = \mathcal{O}_Y$, LHS is $L|_Y \otimes [-1]^* L|_Y$.

1.5.4 In which Rabbit sets out on a long journey to prove finiteness of $H(D)$ implies $|2D|$ is basepoint free and gives a finite map $X \to \mathbf{P}^N$

Note 1.5.5 $|2D|$ is always basepoint free.

Apply the theorem of the square 1.4.15: $T^*_{x+y}D + D \cong T^*_x D + T^*_y D$, let $y = -x$, $2D \cong T^*_x D + T^*_{-x}D$. ($D$ effective) For any $y \in X$, choose some x s.t. RHS doesn't contain y. $E = 2D$

$$\psi_E \colon X \to \mathbf{P}^N$$

can we make this finite? If ψ_E is not finite then $\psi(C) = \text{pt}$ for some irreducible curve C (Zariski's main theorem). For each divisor in $|E|$ either it contains C or fails to intersect C by changing E if necessary, assume $E \cap C = \emptyset$.

Claim 1.5.6 *$T^*_x E \cap C = \emptyset$ or all of C for all $x \in X$.*

Proof. Intersection numbers are constant. ■

Proof. $\mathcal{O}(T^*_x E)|_{\widetilde{C}}$, when $x = 0$ this is trivial so $\deg = 0$. So $\deg = 0$ for all line bundles. E effective implies $C \cap T^*_x E = \emptyset$ for all x s.t. $\cap$ is not in C. ■

Claim 1.5.7 *E is invariant by translation by $x - y$ for $x, y \in C$.*

Proof. If $e \in E$, $T^*_{x-e}(E) \cap C \neq \emptyset$. This is as x is in it, $x - (x - e) = e$, because it is nonempty it's all of C. So y is in it. So $y - (x - e) \in E$. This is also $e - (x - y) \in E$, so E is invariant under T^*_{x-y} ■

Now assume $H(E) = \{x \in X : T^*_x E = E\}$ is finite. But if $\psi_E(C) = \text{pt}$ then $T^*_{x-y}(E) = E$ for all $x, y \in C$. So H is not finite, a contradiction. So ψ_E can't collapse a curve so ψ_E is finite.

1.5.5 In which Piglet discovers a corollary

Corollary 1.5.8 *Abelian varieties are projective.*

Proof. Let X be an abelian variety, $U \subseteq X$ be an open affine set, $0 \in U$, $X \setminus U = D_1 \cup \cdots \cup D_t$ irreducible divisors. Let $D = \sum D_i$, then claim: $H(D) = \{x \in X : T^*_x D = D\}$ is finite. If $H \subseteq U$, U affine, then H closed subvariety of an abelian variety, hence complete, so its finite. If $x \in H$ then $-x \in H$. Now claim that if $x \in H$ then T^*_x preserves U, if not let $u \in U$. Suppose $u - x = d$ for some $d \in D$ then $u = d + x$ which is d translated by $-x$ so $d + x \in D$ so $u \in D$. But contradiction, oh no! So T^*_x preserves U, for all $x \in H$, as $0 \in U$, for all $x \in H$ we have $0 - x \in U$ and $0 + x \in U$ so $H \subseteq U$. ■

Corollary 1.5.9 *Abelian varieties are divisible. $X[n]$ is finite for $n \geq 1$.*

Proof. $[n] \colon X \to X$ and $X[n]$ is the kernel of this. Note that for $x \in X[n]$

$$[n] \circ T_x = [n]$$

$y \in X$, then $n(y - x) = ny - nx = ny$ so for all $L \in \operatorname{Pic} X$

$$T^*_x([n]^* L) \cong ([n]^* L)$$

which implies

$$K([n]^* L) \supseteq X[n]$$

and we just need to find L s.t. this is finite. X projective implies there exists an ample L. The theorem of the cube 1.4.11 implies

$$[n]^*L \cong L^{\frac{n^2+n}{2}} \otimes L^{\frac{n^2-n}{2}}$$

where both terms on the right are ample, hence the left is also. ■

1.5.6 Epilogue: In which we might discuss isogenies

Definition 1.5.10 $f\colon X \to Y$ a morphism of varieties, get a field extension $k(X)/f^*k(Y)$, if $\dim X = \dim Y$ and f is surjective. Then this is a finite field extension and $\deg f$ is $d = [k(X) : f^*k(Y)]$ and $d = \# f^{-1}(y)$ for almost all y. ◊

Definition 1.5.11 A homomorphism of abelian varieties $f\colon X \to Y$ is an **isogeny** if f is surjective with finite kernel. ◊

Corollary 1.5.12 *Degree of* $[n]$ *is* n^{2g}*, if* n *is prime to the characteristic of* k*,* $k = \overline{k}$*,* $g = \dim X$*.*

Proof. Let D be an ample symmetric divisor, e.g.

$$D = D' + [-1]^*D'$$

know $[n]^*D \sim n^2 D$

$$\deg([n]^*(D \cdot \ldots \cdot D)) = ([n]^*D \cdot \ldots \cdot [n]^*D) = (n^2 D \cdot \ldots \cdot n^2 D) = n^{2g}(D \cdot \ldots \cdot D).$$ ■

1.6 Line Bundles and the Dual Abelian Variety (Angus)

1.6.1 Introduction

Meta-goal. Understand line bundles on abelian varieties.

Setup. A an abelian variety $/k$.

Last time. For L a line bundle on A we get a map

$$\begin{aligned} \phi_L\colon A(K) &\longrightarrow \mathrm{Pic}(A) \\ a &\mapsto t_a^*L \otimes L^{-1} \end{aligned}$$

where

$$\mathrm{Pic}(A) = \{\text{line bundles on } A\}/\sim .$$

This a is a group homomorphism (by the theorem of the square 1.4.15). We define

$$K(L)(k) = \ker(\phi_L) = \{a \in A(k) : t_a^*L \simeq L\}.$$

Today. We are going to package these into a big map

$$\begin{aligned} \phi\colon \mathrm{Pic}(A) &\longrightarrow \mathrm{Hom}(A(k), \mathrm{Pic}(A)) \\ L &\mapsto \phi_L. \end{aligned}$$

Proposition 1.6.1

1. *ϕ is a group homomorphism*
2. $$\phi_{t_a^*L} = \phi_L$$

Proof. 1.

$$\begin{aligned}\phi_{L\otimes M}(a) &= t_a^*(L\otimes M)\otimes(L\otimes M)^{-1}\\ &= t_a^*L\otimes L^{-1}t_a^*M\otimes M^{-1}\\ &= \phi_L\otimes\phi_M\end{aligned}$$

2.

$$\begin{aligned}\phi_{t_b^*L}(a) &= t_a^*(t_b^*L)\otimes(t_b^*L)^{-1}\\ &= t_{a+b}^*L\otimes(t_b^*L)^{-1}\\ &= t_a^*L\otimes t_b^*L\otimes L^{-1}\otimes(t_b^*L)^{-1}\\ &= \phi_L(a)\end{aligned}$$

by the theorem of the square 1.4.15 ■

Definition 1.6.2

$$\begin{aligned}\mathrm{Pic}^0(A) &= \ker(\phi)\\ &= \{L\in\mathrm{Pic}(A) : \phi_L = 0\}\\ &= \{L\in\mathrm{Pic}(A) : t_a^*L\simeq L\ \forall a\in A(k)\}\\ &= \{\text{translation invariant line bundles}\}/\!\sim\end{aligned}$$

◊

Goals. Study $\mathrm{Pic}^0(A)$, give it an abelian variety structure, solve a moduli problem, demonstrate some duality.

1.6.2 Aside: alternate description of $\mathrm{Pic}^0(A)$

Definition 1.6.3 Algebraic Equivalence. Two line bundles L_1, L_2 on an abelian variety are **algebraically equivalent** if there exists a variety Y with line bundle L on $A\times Y$ and points $y_1y_2\in Y$ s.t. $L|_{A\times\{y_1\}}\simeq L_1$, $L|_{A\times\{y_2\}}\simeq L_2$. ◊

Remark 1.6.4 This looks like homotopy.

Proposition 1.6.5

$$\mathrm{Pic}^0(A) = \{\textit{line bundles which are alg. equiv to } \mathcal{O}_A\}$$

Proof. [55]. ■

1.6.3 See-Saws

Theorem 1.6.6 See-saw theorem. *Let X, T be varieties X complete, let L be a line bundle on $X\times T$, let $T_1 = \{t\in T : L|_{X\times\{t\}}$ is trivial$\}$ then T_1 is closed in T. Further let $p_2\colon X\times T_1\to T_1$, then $L|_{X\times T_1}\cong p_2^*M$ for some line bundle M on T_1.*

Remark 1.6.7 In fact $M = p_{2*}L$.

Corollary 1.6.8 that no one states/only Milne. *Let X, T be as above and let L, M be line bundles on $X \times T$ s.t.*

$$L|_{X\times\{t\}} \cong M|_{X\times\{t\}} \forall t \in T$$

$$L|_{\{t\}\times X} \cong M|_{\{t\}\times X} \text{ for some } x \in X$$

then $L \cong M$.

1.6.4 Properties of $\operatorname{Pic}^0 A$

Lemma 1.6.9 *$L \in \operatorname{Pic}^0(A)$ and $m, p_1, p_2 \colon A \times A \to A$*

1. $$m^*L \cong p_1^*L \otimes p_2^*L$$
2. *Given $f, g \colon X \to A$* $$(f+g)^*L \cong f^*L \otimes g^*L$$
3. $$[n]^*L \cong L^{\otimes n}$$
4. $$\phi_L(A(k)) \subseteq \operatorname{Pic}^0(A)$$ *for $L \in \operatorname{Pic}(A)$.*

Proof. 1.
$$(m^*L \otimes (p_1^*l)^{-1} \otimes (p_2^*l)^{-1})|_{A\times\{a\}} = t_a^*L \otimes L^{-1} = \mathcal{O}_A$$
$$(m^*L \otimes (p_1^*l)^{-1} \otimes (p_2^*l)^{-1})|_{\{a\}\times A} = t_a^*L \otimes L^{-1} = \mathcal{O}_A$$
by see-saw 1.6.6 whole thing is trivial on $A \times A$.

2.
$$(f+g)^*L \cong (f \times g)^* m^*L \cong (f \times g)^*(p_1^*L \otimes p_2^*L) \cong f^*L \otimes g^*L$$

3. Induction of 3.

4.
$$\phi_{\phi_L(a)} = \phi_{t_a^*L} \otimes L^{-1} = \phi_{t_a^*L} \otimes L^{-1} = \phi_L \otimes \phi_{L^{-1}} = 0$$ ■

Proposition 1.6.10 *If L is nontrivial in $\operatorname{Pic}^0(A)$ then $H^i(A, L) = 0\ \forall i$.*

Proof. If $H^0(A, L) \neq 0$, we would have a nontrivial section s of L then $[-1]^*s$ is a nontrivial section of $[-1]^*L = L^{-1}$. But if both L and L^{-1} have a nontrivial section then $L \cong \mathcal{O}_A$. So since L is nontrivial $H^0(A, L) = 0$. Now assume $H^i(A, L) = 0$ for all $i < j$. Consider

$$A \xrightarrow{\mathrm{id}\times 0} A \times A \xrightarrow{m} A$$
$$a \mapsto (a, 0) \mapsto a$$

this gives
$$H^j(A, L) \to H^j(A \times A, m^*L) \to H^j(A, L)$$

which composes to the identity.

$$H^j(A \times A, m^*L) = H^j(A \times A, p_1^*L \otimes p_2^*L) = \bigoplus_{i=0}^{j} H^i(A, L) \otimes H^{j-i}(A, L)$$

by Künneth. The RHS is 0 by the inductive hypothesis. So the identity on $H^j(A, L)$ factors through 0, hence the group is 0. ■

We now think of ϕ_L as a map $\phi_L : A(k) \to \mathrm{Pic}^0(A)$ with kernel $K(L)(k)$.

Theorem 1.6.11 *If $K(L)(k)$ is finite then ϕ_L is surjective.*

Proof. Idea is to study

$$\Lambda(L) = m^*L \otimes (p_1^*L)^{-1} \otimes (p_2^*L)^{-1}.$$ ■

Given an ample line bundle L on A we now have an isomophism of groups

$$A(k)/K(L)(k) \cong \mathrm{Pic}^0(A)$$

the LHS allows us to put an abelian variety structure on $\mathrm{Pic}^0(A)$.

1.6.5 The Dual Abelian Variety

Theorem 1.6.12 *Let A be an abelian variety and L an ample line bundle on A, then the quotient scheme $A/K(L)$ exists and is an abelian variety of the same dimension as A.*

Proof. (Sketch) (characteristic 0) Cover A by affine opens $U_i = \mathrm{Spec}\, R_i$ such that for all $a \in A$ the orbit $K(L)a \subseteq U_i$ for some i. We can do this because abelian varieties are projective. Then we say $U_i/K(L) = \mathrm{Spec}(R_i^{K(L)})$ then glue. (details in Mumford, II sec, 6 appendix). Since we are in characteristic 0, the quotient scheme is in fact a variety. ■

Definition 1.6.13 Dual abelian varieties. The **dual abelian variety** is

$$\hat{A} = A/K(L).$$

◊

Remark 1.6.14

- $$\hat{A}(K) = \mathrm{Pic}^0(A)$$
- We have an isogeny
$$\phi_L : A \to \hat{A}.$$

Theorem 1.6.15 *There is a unique line bundle $\mathcal{P}$ on $A \times \hat{A}$ called the **Poincaré bundle** such that*

1. $$\mathcal{P}\,|_{A\times\{x\}} \in \mathrm{Pic}^0(A) \textit{ for all } x \in \hat{A}$$
2. $$\mathcal{P}\,|_{0\times\hat{A}} = 0$$
3. *If Z is a scheme with a line bundle R on $A \times Z$ satisfying 1., 2., there exists a*

unique

$$f\colon Z \to \hat{A}$$

s.t.

$$(\mathrm{id} \times f)^* \mathcal{P} = R.$$

That is $(\hat{A}, \mathcal{P})$ *represents the functor*

$$Z \mapsto \left\{ L \in \mathrm{Pic}(A \times Z) : {}^{L|_{A\times\{z\}} \in \mathrm{Pic}^0(A) \forall z \in Z}_{L|_{0\times Z}=0} \right\} /\sim .$$

1.6.6 Dual morphisms

Let $f\colon A \to B$ be a homomorphism of abelian varieties. Let $\mathcal{P}_A, \mathcal{P}_B$ be the Poincaré bundles on A and B. Consider $M = (F \times \mathrm{id}_{\hat{B}})^* \mathcal{P}_B$ on $A \times \hat{B}$, then

1. $$M|_{A\times\{x\}} \in \mathrm{Pic}^0(A)$$

2. $$M|_{\{0\}\times\hat{B}} = 0$$

thus by the universal property we get a unique morphism

$$\hat{f}\colon \hat{B} \to \hat{A}$$

satisfying

$$(\mathrm{id}_A \times \hat{f})^* \mathcal{P}_A = (f \times \mathrm{id}_{\hat{B}})^* \mathcal{P}_B \,.$$

Definition 1.6.16 Dual morphisms. $\hat{f}$ as above is called the **dual morphism**. ◊

Remark 1.6.17

- $$\hat{f}\colon \hat{B} = \mathrm{Pic}^0(B) \to \hat{A}(k) = \mathrm{Pic}^0(A)$$
$$L \mapsto f^* L$$

- $$[\hat{n_A}] = [n_{\hat{A}}]$$

Consider the Poincaré bundle $\mathcal{P}_{\hat{A}}$ on $\hat{A} \times \hat{\hat{A}}$, now think of $\mathcal{P}_A$ as living on $\hat{A} \times A$. By the universal property of $\mathcal{P}_{\hat{A}}$ get a unique morphism

$$\mathrm{can}_A\colon A \to \hat{\hat{A}}.$$

Theorem 1.6.18 can_A *is an isomorphism.*

Lemma 1.6.19

$$\phi_{f^*L} = \hat{f} \circ \phi_L \circ f.$$

Proposition 1.6.20 *If* $f\colon A \to B$ *is an isogeny, then* $\hat{f}\colon \hat{B} \to \hat{A}$ *is an isogeny. Further if* $N = \ker f$*, then* $\hat{N} = \ker \hat{f}$ *is the Cartier dual of* N*.*

Definition 1.6.21 Symmetric morphisms, (principal) polarizations. A morphism $f\colon A \longrightarrow \hat{A}$ is **symmetric** if $f = \hat{f} \circ \mathrm{can}_A$
A **polarization** is a symmetric isogeny $f\colon A \longrightarrow \hat{A}$ s.t. $f = \phi_L$ for some ample line bundle L on A.
A **principal polarization** is a polarization of degree 1, i.e. an isomorphism. ◊

Remark 1.6.22 Elliptic curves always admit principal polarization.
If one wishes to mimic the theory of elliptic curves, one should study principally polarized abelian varieties.

1.7 Endomorphisms and the Tate module (Berke)

Motivation.

$$\begin{aligned} f\colon \mathbf{P}^n \subseteq V_1 &\longrightarrow V_2 \subseteq \mathbf{P}^m,\ V_i = V(I_i) \\ P &\mapsto \cdots \end{aligned}$$

$$f = [f_1 : \cdots : f_m],\ f_i \in \overline{K}(V_1)$$

this feels quite restrictive, an isogeny is even more so, rational, regular, homomorphism, surjective, finite kernel. It feels like there won't be too many but we have multiplication by n etc. so we should ask how many are there that will surprise us? I.e. what is

$$\mathrm{rank}_{\mathbf{Z}} \operatorname{Hom}(A, B) = ?$$

Notation: A, B, C, A_i, B_i are all abelian varieties. $l \neq \operatorname{char} k$, $\sim$ is isogeny.

1.7.1 Poincaré's complete reducibility theorem

Theorem 1.7.1 Poincaré's complete reducibility theorem. *Let $B \subseteq A$ then there is $C \subseteq A$ s.t. $B \cap C$ is finite and $B + C = A$. I.e. $B \times C \longrightarrow A$, $(b, c) \mapsto b + c$ is an isogeny.*

Proof. Choose $\mathcal{L}$ ample on A

$$\begin{tikzcd} B \arrow[r, "i"] \arrow[d, "\phi_{i^*\mathcal{L}}"'] & A \arrow[d, "\phi_{\mathcal{L}}", "\sim"'] \\ \hat{B} & \hat{A} \arrow[l, "\hat{i}"'] \end{tikzcd}$$

C is defined to be the connected component of $\phi_{\mathcal{L}}^{-1}(\ker \hat{i})$ in A

$$\dim C = \dim \ker \hat{i} \geq \dim \hat{A} - \dim \hat{B} = \dim A - \dim B.$$

$B \cap C$ finite, $z \in B$, $z \in B \cap \phi_{\mathcal{L}^{-1}}(\ker \hat{i}) = T_z^* \mathcal{L} \otimes \mathcal{L}^{-1}|_B$ is trivial if and only if $z \in K(\mathcal{L}|_B)$. So $\mathcal{L}|_B$ ample implies $K(\mathcal{L}|_B)$ finite and so $B \cap C$ is finite. So $B \times C \longrightarrow A$ has finite kernel and

$$\dim(B \times C) = \dim B + \dim C \geq \dim A$$

and surjective implies its an isogeny. ∎

Definition 1.7.2 Simple abelian varieties. A is called **simple** if there does not exists $B \subsetneq A$ other than $B = 0, A$. ◊

Corollary 1.7.3

$$A \sim A_1^{n_1} \times \cdots \times A_k^{n_k}$$

$A_i \nsim A_j$ for $i \neq j$ and A_i simple.

Corollary 1.7.4 *$\alpha \in \operatorname{Hom}(A, B)$ for A, B simple then α is an isogeny or 0.*

Proof. $\alpha(A) \subseteq B$ which implies $\alpha(A) = B$ or 0. The connected component of 0 of $\ker \alpha$ will be an abelian subvariety of A, denote it C If $C = 0$ then $\ker \alpha$ is finite, if $C = A$ then $\alpha = 0$. So α is an isogeny or 0. ■

Corollary 1.7.5 *If A, B are simple and $A \nsim B$ then $\operatorname{Hom}(A, B) = 0$.*

Definition 1.7.6

$$\operatorname{End}^0(A) = \operatorname{End}(A) \otimes \mathbf{Q}.$$

◊

Lemma 1.7.7 *If $\alpha \colon A \longrightarrow B$ is an isogeny, then there exists $\beta \colon B \longrightarrow A$ s.t. $\beta \circ \alpha = n_A$ for some $n \geq 1$.*

Proof. α an isogeny implies $\ker \alpha$ is finite. So there exists n with $n \ker \alpha = 0$. $\ker \alpha \subseteq \ker n_A$

$$\begin{tikzcd}
& A \arrow[r, "n_A"] \arrow[dl, "\alpha"'] \arrow[d] & A \\
B \arrow[r, "\sim"'] \arrow[urr, bend right=70] & A/\ker\alpha \arrow[ur, "\circ"'] \arrow[d, "\exists|\beta"] & \\
& A/n_A &
\end{tikzcd}$$

so $\beta \circ \alpha = n_A$, also $\alpha \circ \beta = n_B$. ■

Corollary 1.7.8 *A is simple then $\operatorname{End}^0(A)$ is a division ring, $\alpha^{-1} = \beta \otimes \frac{1}{n}$.*

Corollary 1.7.9 to Poincaré reducibility theorem. *If*

$$A \sim A_1^{n_1} \times \cdots \times A_k^{n_k}$$

then

$$\operatorname{End}^0(A) \simeq \prod \operatorname{End}^0(A_i)^{n_i^2}.$$

Proof.

$$\begin{aligned}
\operatorname{End}(A) \otimes \mathbf{Q} &\simeq \prod_{i,j} \operatorname{Hom}(A_i^{n_i}, A_j^{n_j}) \otimes \mathbf{Q} \\
&\simeq \prod_i \operatorname{End}(A_i)^{n_i^2} \otimes \mathbf{Q} \\
&\simeq \prod_i \operatorname{End}^0(A_i)^{n_i^2}
\end{aligned}$$

■

Theorem 1.7.10 7.2. *If $\dim A = g$ then $\deg n_A = n^{2g}$.*

Corollary 1.7.11 *$\operatorname{char} k \nmid n$ implies $\ker(n_A) \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$.*

Proof. If $m|n$ then $|\ker(m_A)| = m^{2g}$, then use structure theorem. ∎

In particular if we let $A[l^n] = A(k^{\text{sep}})[l^n]$, then $A[l^n] \simeq (\mathbf{Z}/l^n)^{2g}$ Define

$$T_l(A) = \varprojlim_n A[l^n],\ A[l^{n+1}] \xrightarrow{l} A[l]$$

Proposition 1.7.12
$$T_l \simeq (\mathbf{Z}_l)^{2g}$$

$\alpha\colon A \to B$ induces
$$T_l\alpha\colon T_l(A) \to T_l(B)$$
$$(a_1, a_2, \ldots) \mapsto (\alpha(a_1), \alpha(a_2), \ldots)$$

Lemma 1.7.13
$$\operatorname{Hom}(A,B) \hookrightarrow \operatorname{Hom}(T_l(A), T_l(B))$$

Proof. Let $\alpha \in \operatorname{Hom}(A,B)$ and assume $T_l\alpha = 0$ then

$$\ker(\alpha|_{A_i}) \supseteq A_i[l^n] \forall n$$

for any simple component A_i of A so $\alpha = 0$ on each A_i and hence $\alpha = 0$ on A. ∎

Corollary 1.7.14 $\operatorname{Hom}(A,B)$ *is torsion free.*

Recall we are interested in knowing about $\operatorname{rank}_{\mathbf{Z}} \operatorname{Hom}(A,B)$ =?, can we bound this? If we could show that

$$\operatorname{Hom}(A,B) \otimes \mathbf{Z}_l \hookrightarrow \operatorname{Hom}(T_l(A), T_l(B))$$

we could conclude, so:

$$\begin{tikzcd} \operatorname{Hom}(A,B)\otimes \mathbf{Z}_l \arrow[r, hook] \arrow[d, "\sim"'] & \operatorname{Hom}(T_lA, T_lB) \arrow[d, "\sim"'] \\ \prod_{i,j}(\operatorname{Hom}(A_i,B_j)\otimes \mathbf{Z}_l) \arrow[r, hook] & \prod_{i,j}\operatorname{Hom}(T_lA_i, T_lB_j) \end{tikzcd}$$

$A_i + B_j = 0$, $A_i \sim B_j$ $\operatorname{Hom}(A_i, B_j) \hookrightarrow \operatorname{End}(A_i)$. Assume $A = B$ and A simple, then $\operatorname{End}(A) \otimes \mathbf{Z}_l \hookrightarrow \operatorname{End}(T_l(A))$.

Definition 1.7.15 V/k then $f\colon V \to k$ is called a (homogenous) polynomial function of degree d if $\forall\{v_1, \cdots, v_m\} \subseteq V$ linearly independent.

$$f(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m)$$

is given by a homogenous polynomial of degree d in λ_i i.e.

$$f(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m) = P(\lambda_1, \ldots, \lambda_m)$$

for some $P \in k[X_m]$ homogenous of degree d. ◊

$$\deg\colon \operatorname{End}(A) \to \mathbf{Z}$$

α an isogeny iff $\deg\alpha$, α not an isogeny iff 0.

Theorem 1.7.16 deg *uniquely extends to a polynomial function of degree* $2g$ *on* $\operatorname{End}^0(A) \to \mathbf{Q}$.

Proof. (of above continued)

$$\mathrm{End}(A) \otimes \mathbf{Z}_l \hookrightarrow \mathrm{End}(T_l(A))$$

for A simple iff for any finitely generated $M \subseteq \mathrm{End}(A)$

$$M \otimes \mathbf{Z}_l \hookrightarrow \mathrm{End}(T_l(A))$$

Claim:

$$M^{\mathrm{div}} = \{f \in \mathrm{End}(A) : nf \in M \text{ for some } n \geq 1\}$$

is finitely generated.

Proof: $M^{\mathrm{div}} = (M \otimes \mathbf{Q}) \cap \mathrm{End}(A)$ $\deg\colon M \otimes \mathbf{Q} \to \mathbf{Q}$ is a polynomial so it is continuous.

$$U = \{\phi \in M \otimes \mathbf{Q} : \deg \phi < 1\}$$

is open in $M \otimes \mathbf{Q}$ but $U \cap M^{\mathrm{div}} = 0$ so M^{div} is a discrete subgroup of the finite dimensional $\mathbf{Q}$-vector space $M \otimes \mathbf{Q}$ so M^{div} is finitely generated. $M \hookrightarrow M^{\mathrm{div}}$ so $M \otimes \mathbf{Z}_l \hookrightarrow M^{\mathrm{div}} \otimes \mathbf{Z}_l$ so we may assume $M = M^{\mathrm{div}}$.

Let $f_1, \ldots, f_r$ be a $\mathbf{Z}$-basis for M and suppose that $\sum a_i T_l(f_i) = 0$ for some $a_i \in \mathbf{Z}_l$ not all 0. We can assume not all a_i are divisible by l. Choose $a'_i \in \mathbf{Z}$ s.t. $a'_i = a_i \pmod l$

$$f = \sum a'_i f_i \in \mathrm{End}(A)$$

we then have

$$f = \sum a'_i T_l f_i$$

is 0 on the first coordinate of T_l. So $A[l] \subseteq \ker f$ so there exists g with $f = lg$ $f \in M$ implies $g \in M^{\mathrm{div}} = M$ so $g = \sum b_i f_i$ and $f = \sum l b_i f = \sum a_i f_i$ hence $l \mid a_i$ for all i a contradiction. So $\mathrm{End}(A) \otimes \mathbf{Z}_l \hookrightarrow \mathrm{End}(T_l(A))$.

Therefore

$$\mathrm{Hom}(A, B) \otimes \mathbf{Z}_l \hookrightarrow \mathrm{Hom}(T_l(A), T_l(B))$$

$$\mathrm{rank}_{\mathbf{Z}} \mathrm{Hom}(A, B) \leq 4 \dim A \dim B.$$

■

1.8 Polarizations and Étale cohomology (Alex)

Plan: polarizations, a little cohomological warmup and a cool finiteness result. Étale cohomology.

1.8.1 Polarizations

Definition 1.8.1 Polarizations. A **polarization** of an abelian variety A/k is an isogeny

$$\lambda\colon A \to \hat{A}$$

such that

$$\lambda \simeq_{\overline{k}} \lambda_{\mathcal{L}} : a \mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

for an ample invertible sheaf $\mathcal{L}$ on $A_{\overline{k}}$.

We then have a notion of degree, polarizations of degree 1 (i.e. isomorphisms $A \to \hat{A}$) are called **principal polarizations**. ◊

Remark 1.8.2 This is in fact equivalent to the previous definition 1.6.21, see [70, cor. 11.5].

Natural questions: what does the line bundle $\mathcal{L}$ tell us about the polarization? Can we tell principality?

To answer this we must (rapidly) recall (Zariski) sheaf cohomology. But this will help us in the next section too.

A line bundle (or indeed any sheaf) defines for us for any open subset $U \hookrightarrow X$ an abelian group of sections $\mathcal{L}(U)$.

However taking (global) sections doesn't play well with exact sequences!

Example 1.8.3 Classic example. Let $X = \mathbf{C}^*$ and consider

$$0 \to \mathbf{Z} \hookrightarrow \mathcal{O}_X \xrightarrow{e^{2\pi i -}} \mathcal{O}_X^* \to 0$$

but

$$0 \to \mathbf{Z} \to \mathcal{O}_X(X) \to \mathcal{O}_X^*(X)$$

is not surjective on the right, for example $f(z) = z$ is a nowhere vanishing meromorphic function on X but its not exp of anything. Upshot: maps of sheaves can be surjective (by being so locally) but not globally. □

To understand/control this phenomenon we introduce $H^1(X, \mathcal{F})$ fitting into the above and so on.

Explicitly: for a sheaf $\mathcal{F}$ we fix an injective resolution

$$0 \to \mathcal{F} \to \mathcal{I}_0 \to \mathcal{I}_1 \to \cdots$$

which we then take global sections of to get a chain complex

$$0 \to \Gamma(X, \mathcal{F}) \to \Gamma(X, \mathcal{I}_0) \to \Gamma(X, \mathcal{I}_1) \to \cdots$$

and we truncate and take cohomology of this to measure "failure of exactness"

$$H^0(X, \mathcal{F}), H^1(X, \mathcal{F}), H^2(X, \mathcal{F}), \ldots.$$

Definition 1.8.4 Euler-Poincaré characteristic. Define the **Euler-Poincaré characteristic** of a line bundle $\mathcal{L}$ to be

$$\chi(\mathcal{L}) = \sum (-1)^i \dim_k H^i(A, \mathcal{L}).$$

◊

Theorem 1.8.5 Riemann-Roch. *Let A be an abelian variety of dimension g then*

1. *The degree of $\lambda_{\mathcal{L}}$ is $\chi(\mathcal{L})^2$.*
2. *If $\mathcal{L} = \mathcal{L}(D)$ then $\chi(\mathcal{L}) = (D^g)/g!$, this is the g-fold self intersection number of D.*

Theorem 1.8.6 Vanishing. *If $\#K(\mathcal{L}) < \infty$ then there is a unique integer $0 \le i(\mathcal{L}) \le g$ with $H^i(A, \mathcal{L}) \ne 0$ and $H^p(A, \mathcal{L}) = 0$ for all $p \ne i$. Moreover $i(\mathcal{L}^{-1}) = g - i(\mathcal{L})$.*

Recall Subsection 1.5.3: So for ample $\mathcal{L}$ we have $K(\mathcal{L})$ finite, so the vanishing theorem applies. Additionally for very ample $\mathcal{L}$ we know $H^0(A, \mathcal{L}) \ne 0$ so in this case we get vanishing of higher cohomology.

Theorem 1.8.7 Finiteness. *Let k be a finite field, and $g, d \ge 1$ integers. Up to isomorphism there are only finitely many abelian varieties A/k of dimension g and with a polarization of degree d^2.*

Proof. (Super sketch)

Over a finite field implies there is an ample $\mathcal{L}$ with $\lambda_{\mathcal{L}}$ a polarization of degree d^2, then using above $\chi(\mathcal{L}^3) = 3^g d$ and $\mathcal{L}^3$ is very ample hence $\dim H^0(A, \mathcal{L}^3) = 3^g d$ so we get an embedding into $\mathbf{P}^{3^g d-1}$.

The degree of A in $\mathbf{P}^{3^g d-1}$ is $((3D)^g) = 3^g d(g!)$. It is determined by its Chow form, which by these formulae has some (large) bounded degree, as we are over a finite field however there are only finitely many such. ■

1.8.2 Étale Cohomology of Abelian Varieties

See [51] or [67].

Recall for abelian varieties over $A/\mathbf{C}$ we considered singular cohomology of the complex points $A(\mathbf{C})$. Indeed this theory was strongly connected to the lattice Λ defining $A(\mathbf{C})$.

We saw that in fact $\pi_1(A, 0) = \pi^{-1}(0) = \Lambda \subseteq V$ which was the universal covering space of $A(\mathbf{C})$. We want to emulate this over a general field.

We want to allow multiplication by n to define finite covers for our abelian varieties as they did before.

Problem: Zariski topology is too coarse: we can't find an open U set around $0 \in A$ such that $[2]\colon U \to A$ is an isomorphism onto its image. Isogenies are not local isomorphisms for the Zariski topology.

How on earth do we "allow" maps which are clearly not local isomorphisms to become such? First what do we mean by local isomorphism?

$$\begin{tikzcd} f^{-1}(U) \arrow[r, "\sim"] \arrow[d] & U \arrow[d, hook, "i"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}.$$

There exists an open subset U such that the base change $X \times_Y U$ is isomorphic with $\coprod U$ of several copies of U in a compatible way with the map to U.

So let's cheat, the best isomorphism is the identity map

$$\begin{tikzcd} X \arrow[r, "\sim"] \arrow[d] & X \arrow[d, "f"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

if we define an "open set" U to be a morphism $X \to Y$ with the properties we want, then all such become local isomorphisms.

By taking our *topology* to be given by some maps we decide are decent covering maps we can circumvent these difficulties.

What is the correct class of morphisms to take here, we feel like our $[n]$ maps should count. Taking inspiration from differential geometry perhaps, we are led to the notion of a local diffeomorphism, an étale map.

Definition 1.8.8 Let X, Y be nonsingular varieties over $k = \overline{k}$. Then $f\colon X \to Y$ is étale at a point $P \in X$ if

$$\mathrm{d}f\colon \operatorname{Tgt}_P(X) \to \operatorname{Tgt}_{f(P)}(Y)$$

is an isomorphism. ◊

Proposition 1.8.9 *Let $f\colon \mathbf{A}^m \to \mathbf{A}^m$ then f is étale at $(a_1, \cdots, a_m)$ iff*

$$\left(\frac{\partial(X_i \circ f)}{\partial Y_j}|_{(a_k)}\right)$$

is nonsingular.

Example 1.8.10 A non-étale map. Consider the map

$$\mathbf{A}^2 \to \mathbf{A}^2$$
$$(x, y) \mapsto (x^3, x^2 + y)$$

we can see that the image of $y = 0$ is the nodal cubic ($Y^3 = X^2$), which is messed up (singular) at $(0, 0)$. The jacobian is

$$\begin{pmatrix} 3x^2 & 0 \\ 2x & 1 \end{pmatrix}$$

so this matrix is singular exactly when $x = 0$ (unless characteristic 3). So the map is not étale at these points. □

Proposition 1.8.11 *The maps $[n]$ are étale on an abelian variety A/k for all $\operatorname{char} k \nmid n$*

Proof. Key point $\mathrm{d}(\alpha + \beta)_0 = (\mathrm{d}\alpha)_0 + (\mathrm{d}\beta)_0$. So the map on tangent spaces is simply multiplication by n. ■

Definition 1.8.12 Étale morphisms. A morphism $f\colon X \to Y$ of schemes is **étale** if it is flat and unramified.
Flatness for finite morphisms of varieties is equivalent to each fibre $f^{-1}(t)$ being of equal cardinality, counting multiplicities. ◊

All isogenies are finite and flat.

Definition 1.8.13 Let FEt/X be the category of finite étale maps $\pi\colon Y \to X$ (i.e. finite étale coverings of X).
Then after picking a basepoint $x \in X$ we can map

$$F\colon \mathrm{FEt}/X \to \mathrm{Set}$$

$$\pi \mapsto \mathrm{Hom}_X(x, Y) \approx \pi^{-1}(x).$$

This is in fact pro-representable, i.e. there exists a system

$$\tilde{X} = (X_i)_{i\in I}$$

with

$$F(Y) = \mathrm{Hom}(\tilde{X}, Y) = \varinjlim_i \mathrm{Hom}(X_i, Y).$$

We then define

$$\pi_1(X, x) = \mathrm{Aut}_X(\tilde{X}) = \varprojlim_i \mathrm{Aut}_X(X_i).$$

◊

So we need to understand étale covers of abelian varieties. Following [70]:

Proposition 1.8.14 surprising proposition. *Let X be a complete variety over a field k with $e \in X(k)$ and $m\colon X \times X \to X$ s.t. $m(e, x) = m(x, e) = x$ for all $x \in X$. Then (X, m, e) is an abelian variety.*

Proof. (Sketch)

Let

$$\tau\colon X \times X \to X \times X$$
$$\tau(x, y) = (xy, y)$$

so $\tau^{-1}(e, e) = (e, e)$. Some exercise in Hartshorne implies $\operatorname{im}\tau$ has dimension $2\dim X$.

Reduce to algebraically closed case.

Let

$$\tau^{-1}(\{e\} \times X) = \{(x, y) : xy = e\} = \Gamma \subseteq X \times X$$

as τ is surjective we get $p_2\colon \Gamma \to X$ is also so pick an irreducible $\Gamma_1 \subseteq \Gamma$ with $p_2(\Gamma_1) = X$. This also implies $p_1(\Gamma_1) = X$.

Let

$$f\colon \Gamma_1 \times X \times X \to X$$
$$f((x, y), z, w) = x((yz)w)$$

then

$$f(\Gamma_1 \times \{e\} \times \{e\}) = \{eee\} = \{e\}$$

so a version of rigidity 1.1.11 gives

$$x((yz)w) = zw \;\forall (x, y) \in \Gamma_1,\; z, w \in X$$

So letting $w = e$ we get

$$x(yz) = z.$$

Fix $y \in X(k)$, and then by surjectivity we can find $x, z \in X(k)$ with $(x, y) \in \Gamma_1 \ni (y, z)$. So we get

$$x = x(yz) = ze = z$$

and so y has both a left and right inverse. We then multiply above by y to get

$$y(zw) = y(x((yz)w)) = (yz)w$$

so $X(k)$ is associative. ∎

Theorem 1.8.15 Lang-Serre. *Let X/k be an abelian variety and Y/k a variety with $e_Y \in Y(k)$ s.t. $f\colon Y \to X$ is an étale covering where $f(e_Y) = e_X$. Then Y can be given the structure of an abelian variety so that f is a separable isogeny.*

Proof. Must construct a group law on Y:

Take the graph of $m\colon X \times X \to X$

$$\Gamma_X \subseteq X \times X \times X$$

and pullback along $f \times f \times f$ to

$$\Gamma'_Y \subseteq Y \times Y \times Y$$

fix the connected component Γ_Y containing (e_Y, e_Y, e_Y).

Call the projections from Γ_Y q_I. Now we must show that $q_{12}\colon \Gamma_Y \to Y \times Y$ is an isomorphism, then $m_Y\colon Y \times Y \to Y$ can be defined as $q_3 \circ q_{12}^{-1}$. q_{12} has sections s_1, s_2 over $\{e_Y\} \times Y$, $Y \times \{e_Y\}$ respectively given by $s_1(e_Y, y) = (e_Y, y, y)$ and $s_2(y, e_y, y) = (y, e_y, y)$. So m_Y satisfies the conditions of the surprising proposition.

$$\begin{tikzcd}
\Gamma_Y \arrow[r] \arrow[d, "q_{12}"'] & \Gamma_X \arrow[d, "p_{12}"] \\
Y \times Y \arrow[r, "f \times f"'] & X \times X
\end{tikzcd}$$

the horizontal maps are étale coverings and the rightmost an isomorphism so q_{12} is an étale covering. The projection $p_2 \circ q_{12} = q_2 \colon \Gamma_Y \to Y$ is smooth proper. Fact: all fibres of q_2 are irreducible. So $Z = q_2^{-1}(e_Y) = q_{12}^{-1}(Y \times \{e_Y\})$ is irreducible. Moreover q_{12} restricts to an étale covering $Z \to Y = Y \times \{e_Y\}$ of the same degree, but s_2 is a section of this covering, hence it is an isomorphism. Hence q_{12} has degree 1 and is therefore an isomorphism as required. ∎

So we have some control over the finite étale maps, what does the covering space look like? Last week we saw that for an isogeny $\alpha \colon B \to A$ we could find $\beta \colon A \to B$ with $\beta \circ \alpha = [n] \colon A \to A$. This means we can take our universal covering space to be

$$(A)_{i \in I}$$

with multiplication by n maps.

So we find

$$\pi_1^{\mathrm{et}}(A, 0) = \varprojlim_n \mathrm{Aut}_A(A \xrightarrow{[n]} A) = \varprojlim_n A[n].$$

Theorem 1.8.16

$$H^1_{\mathrm{et}}(A, \mathbf{Z}_l) = \mathrm{Hom}(\pi_1(A, 0), \mathbf{Z}_l) = \mathrm{Hom}(T_l, \mathbf{Z}_l)$$

Theorem 1.8.17

$$H^r(A_{\mathrm{et}}, \mathbf{Z}_l) = \bigwedge^r H^1(A_{\mathrm{et}}, \mathbf{Z}_l)$$

Note that Milne gives a combined proof of the above two statements, this relies on some theorems on Hopf algebras such as [17, Theoreme 6.1].

1.9 Weil pairings (Maria)

1.9.1 Weil pairings on elliptic curves

Start with elliptic curves, later repeat for abelian varieties. E/k an elliptic curve, $m \geq 2$, if $\mathrm{char}(k) = p > 0$ $(m, p) = 1$. The Weil e_m-pairing $e_m \colon E[m] \times E[m] \to \mu_m$ is defined as follows: Fix $T \in E[m]$ then $f \in \overline{k}(E)$ s.t. $\mathrm{div}(f) = m(T) - m(0)$. Fix $T' \in E$ with $mT' = T$ and $g \in \overline{k}(E)$ s.t. $\mathrm{div}(g) = [m]^*(T) = [m]^*(0) = \sum_{R \in E[m]} (T + R) - (R)$. Check $\mathrm{div}(f \circ [m]) = \mathrm{div}(g^m)$, hence

$$f \circ [m] = c g^m$$

so can assume $f \circ [m] = g^m$. For $s \in E[m]$, $x \in E$:

$$g(x + s) = f([m]x + [m]s) = f([m]x) = g(x)^m$$

$$\frac{g(\cdot + s)^m}{g(\cdot)} \colon E \to \mathbf{P}^1$$

is then a constant function, since not surjective. So we define

$$\begin{aligned} e_m \colon E[m] \times E[m] &\to \mu_m \\ (s, t) &\mapsto \frac{g_t(x + s)}{g_t(x)} \end{aligned}$$

will state many properties later, but for now. e_m is compatible:

$$e_{mm'}(a, a')^{m'} = e_m(m'a, m'a') \; \forall a, a' \in E[mm']$$

so for any $l \neq \mathrm{char}(k)$ prime we can combine e_{l^n}-pairings into an l-adic Weil pairing on $T_l E$

$$e\colon T_l E \times T_l E \longrightarrow T_l \mu = \mathbf{Z}_l(1)$$

1.9.2 Weil pairings on abelian varieties

Story will be broadly similar to before but we must use the dual, which doesn't appear in the presentation for elliptic curves.

Let A/k be an abelian variety $k = \overline{k}$. We construct a Weil e_m-pairing

$$e_m\colon A[m] \times A^\vee[m] \longrightarrow \mu_m$$
$$(a, a') \mapsto \frac{g \circ t_a(x)}{g(x)} = \frac{g(x+a)}{g(x)}$$

Fix $a \in A[m]$, $a' \in A^\vee[m]$ say a' corresponds to $\mathcal{L}$ and a divisor D then $\mathcal{L}^m$ and $m_A^* \mathcal{L}$ are trivial so $\exists f, g \in k(A)$ s.t.

$$\mathrm{div}(f) = mD$$
$$\mathrm{div}(g) = m_A^* D$$

again we have

$$\mathrm{div}(f \circ m_A) = \mathrm{div}(g^m)$$
$$g(x+a)^m = g(x)^m$$

Proposition 1.9.1 *The Weil e_m-pairing has the following properties*

1. *e_m is bilinear*
$$e_m(a_1 + a_2, a') = e_m(a_1, a')e_m(a_2, a')$$
$$e_m(a, a_1' + a_2') = e_m(a, a_1')e_m(a, a_2')$$

2. *e_m is non-degenerate: if $e_m(a, a') = 1 \forall a \in A[m]$ then $a' = 0$ (and likewise for the reverse).*

3. *e_m is Galois-invariant... but we assume $\overline{k} = k$ so we ignore this.*

4. *e_m is compatible*
$$e_{mm'}(a, a')^{m'} = e_m(m'a, m'a') \;\forall a \in A[mm'], a' \in A^\vee[mm']$$
$(mm', \mathrm{char}\, k) = 1$

Corollary 1.9.2 *There exists a bilinear non-degenerate (Galois invariant) pairing*

$$e_l = e\colon T_l A \times T_l A^\vee \longrightarrow T_l \mu$$
$$((a_n), (a_n')) \mapsto (e_{l^n}(a_, a_n'))$$

For a homomorphism $\lambda\colon A \to A^\vee$ we define

$$e_m^\lambda\colon A[m] \times A[m] \longrightarrow \mu_m$$
$$(a, a') \mapsto e_m(a, \lambda(a'))$$
$$e_m\colon T_l A \times T_l A \longrightarrow T_l \mu$$
$$(a, a') \mapsto e_m(a, \lambda(a')).$$

Notation. If $\lambda = \lambda_{\mathcal{L}} e^{\mathcal{L}} = e^{\lambda_{\mathcal{L}}}$.

Proposition 1.9.3 *For a homomorphism $\alpha\colon A \to B$*

1. $$e(a, \alpha^\vee(b)) = e(\alpha(a), b) \forall a \in T_l A,\ b \in T_l B$$

2. $$e^{\alpha^\vee \lambda \alpha}(a, a') = e^\lambda(\alpha(a), \alpha(a'))$$

   for $a, a' \in T_l(A)$, $\lambda \in \mathrm{Hom}(B, B^\vee)$.

3. $$e^{\alpha^* \mathcal{L}}(a, a') = e^{\mathcal{L}}(\alpha(a), \alpha(a'))$$

   $a, a' \in T_l A$ $\mathcal{L} \in \mathrm{Pic}(B)$.

4. $$\mathrm{Pic}\, A \to \mathrm{Hom}(\bigwedge^2 T_l A, T_l \mu)$$
   $$\mathcal{L} \mapsto e^{\mathcal{L}}$$

   is a homomorphism (in particular $e^{\mathcal{L}}$ is skew-symmetric).

Proof.

1. $a = (a_n) \in T_l A$ $b \in (b_n) \in T_l B^\vee$ fix a divisor D on B representing b_n and $g \in k(B)$ s.t. $\mathrm{div}(h) = (l_B^n)^* D$. Then $\alpha^* D$ represents $\alpha^\vee(b_n)$ so:

   $$\mathrm{div}(g \circ \alpha) = \alpha^* \mathrm{div}(g) = \alpha^*(l_B^n)^* D = (l_A^n)^* \alpha^* D.$$

   So

2. $$e^{\alpha^\vee \lambda \alpha}(a, a') = e(a, \alpha^\vee \lambda \alpha(a')) = e(\alpha(a), \lambda(\alpha(a'))) = e^\lambda(\alpha(a), \alpha(a')).$$

3. $$\lambda_{\alpha^* \mathcal{L}} = \alpha^\vee \lambda_{\mathcal{L}} \alpha$$

4. Follows from $\lambda_{\mathcal{L} \otimes \mathcal{L}'} = \lambda_{\mathcal{L}} + \lambda_{\mathcal{L}'}$.

∎

Example 1.9.4 Computation over C. $A/\mathbf{C}$ be an abelian variety

$$0 \to \mathbf{Z} \to \mathcal{O}_A \xrightarrow{e^{2\pi i(\cdot)}} \mathcal{O}^\times \to 0$$

induces

$$H^1(A(\mathbf{C}), \mathbf{Z}) \to H^1(A(\mathbf{C}), \mathcal{O}) \to H^1(A(\mathbf{C}), \mathcal{O}^\times) \simeq \mathrm{Pic}\, A \to H^2(A(\mathbf{C}), \mathbf{Z})$$

and

$$H^1(A(\mathbf{C}), \mathcal{O}) / H^1(A(\mathbf{C}), \mathbf{Z}) \simeq A^\vee(\mathbf{C}) = \mathrm{Pic}^0(A)$$

so we get an exact sequence

$$0 \to \mathrm{NS}(A) \to H^2(A(\mathbf{C}), \mathbf{Z}) \to H^2(A(\mathbf{C}), \mathcal{O}_A)$$

$$\lambda \mapsto E_\lambda$$

then we can regard E_λ as a skew-symmetric 2-form on $H_1(A(\mathbf{C}), \mathbf{Z})$. Mumford pg. 237 proves

$$\begin{tikzcd} H_1(A(\mathbf{C}),\mathbf{Z}) \times H_1(A(\mathbf{C}),\mathbf{Z}) \arrow[r] \arrow[d] & \mathbf{Z} \ni m \arrow[d] \\ T_l \times T_l \arrow[r] & T_l\mu \ni \zeta^m \end{tikzcd}$$

commutes with - sign so $e^\lambda(a,a') = \zeta^{-E(a,a')}$ □

1.9.3 Results about polarizations

$k = \overline{k}$ $p = \mathrm{char}(k) \geq 0$.

Theorem 1.9.5 13.4. *Let $\alpha\colon A \to B$ be an isogeny of degree prime to $\mathrm{char}\, k$ and $\lambda \in \mathrm{NS}(A)$ then $\lambda = \alpha^*\lambda'$ for $\lambda' \in \mathrm{NS}(B)$ $\iff$ $\forall l | \deg(\alpha)$ l prime there exists a skew-symmetric form $f\colon T_lB \times T_lB \to T_l\mu$ s.t. $e^\lambda(a,a') = f(\alpha(a),\alpha(a'))$ for all $a,a' \in T_l(A)$.*

Proof. Milne 1986 16.4 ■

Corollary 1.9.6 13.5. *$l \neq \mathrm{char}(k)$ $\lambda \in \mathrm{NS}(A)$ is divisible by l^n $\iff$ e^λ is divisible by l^n in $\mathrm{Hom}(\bigwedge^2 T_lA, T_l\mu)$.*

Proof. Apply theorem 13.4 with $\alpha = l^n$. ■

Lemma 1.9.7 13.7. *Let $\mathcal{P}$ be the Poincaré sheaf on $A \times A^\vee$ then*

$$e^{\mathcal{P}}((a,b),(a',b')) = \frac{e(a,b')}{e(a',b)}$$

for all $a,a' \in T_lA$, $b,b' \in T_lA^\vee$.

Proof. Milne 1986 16.7. Use:

$$(1+\lambda_{\mathcal{L}})^*\mathcal{P} \cong m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1} \otimes q^*\mathcal{L}^{-1}$$ ■

Proposition 1.9.8 13.6. *Assume $\mathrm{char}\, k \neq l, 2$ then a homomorphism $\lambda\colon A \to A^\vee$ is $\lambda = \lambda_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{Pic}\, A$ iff e^λ is skew-symmetric.*

Proof. Clear.

e^λ is skew-symmetric, define $\mathcal{L} = (1 \times \lambda)^*\mathcal{P}$ then $\forall a,a' \in T_lA$

$$e(a,\lambda_{\mathcal{L}}(a')) = e^{\mathcal{L}}(a,a') = e^{(1\times\lambda)^*\mathcal{P}}(a,a') = e^{\mathcal{P}}((a,\lambda(a)),(a',\lambda(a'))) = \frac{e(a,\lambda(a'))}{e(a',\lambda(a))}$$

$$= \frac{e^\lambda(a,a')}{e^\lambda(a',a)} = (e^\lambda(a,a'))^2 = e(a, 2\lambda(a'))$$

so $2\lambda = \lambda_{\mathcal{L}}$. So by corollary 13.5 $\lambda_{\mathcal{L}} = 2\lambda_{\mathcal{L}'}$ for some $\mathcal{L}' \in \mathrm{Pic}\, A$ so $\lambda = \lambda_{\mathcal{L}'}$. ■

Definition 1.9.9 For a polarization $\lambda\colon A \to A^\vee$ define

$$e^\lambda\colon\ \ker(\lambda) \times \ker(\lambda) \to \mu_m$$

$$(a,a') \mapsto e_m(a,\lambda(b))$$

where m kills $\ker(\lambda)$ and $b \in A$ s.t.$mb = a'$. ◊

Check: this is well defined.

Note 1.9.10 e^λ is skew-symmetric.

Proposition 1.9.11 13.8. *$\alpha\colon A \to B$ is an isogeny of degree prime to p, $\lambda\colon A \to A^\vee$ polarization then $\lambda = \alpha^*\lambda'$, $\lambda'\colon B \to B^\vee$ polarization iff*

$$\ker(\alpha) \subset \ker \lambda$$

$$e^\lambda \textit{ is trivial on } \ker(\alpha) \times \ker(\alpha)$$

Note 1.9.12 If $\lambda = \alpha^*\lambda'$ then

$$\deg(\lambda) = \deg(\lambda')\deg(\alpha)^2.$$

Corollary 1.9.13 13.10. *A an abelian variety, $\lambda\colon A \to A^\vee$ is a polarization with $(\deg(\lambda), p) = 1$ then A is isogenous to a principally polarized abelian variety.*

Proof. Fix $l|\deg(\lambda)$ prime. Choose a subgroup $N \subseteq \ker\lambda$ of order l let $\alpha\colon A \to A/N = B$ N is cyclic and e^λ is skew-symmetric so e^λ is trivial on $N \times N$ so B has a polarization of degree $\deg(\lambda)/l^2$ by 13.8. ∎

Corollary 1.9.14 13.11. *Let λ be a polarization of A s.t. $\ker(\lambda) \subseteq A[m]$ for some $(m, p) = 1$. If $\exists\alpha\colon A \to A$ s.t. $\alpha(\ker(\lambda)) \subseteq \ker(\lambda)$ and $\alpha^\vee\lambda\alpha = -\lambda$ on $A[m^2]$ then $A \times A^\vee$ is principally polarized.*

Theorem 1.9.15 13.12 (Zarhin's trick). *For any abelian variety A $(A \times A^\vee)^4$ is principally polarized.*

Proof. Fix $\lambda\colon A \to A^\vee$ polarization, assume $\ker(\lambda) \subseteq A[m]$ $(m, p) = 1$ there exists $a, b, c, d \in \mathbf{Z}$ s.t. $a^2 + b^2 + c^2 + d^2 = m^2 - 1 = -1 \pmod{m^2}$ then

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

works. ∎

Corollary 1.9.16 13.13. *Let k be a finite field, then for each $g \in \mathbf{Z}$ there exist only finitely many isomorphism classes of abelian varieties of dimension g over k.*

Proof. A/k an abelian variety of dimension g, so $(A \times A^\vee)^4$ is an abelian variety of dimension $8g$ with a principal polarization so using theorem 11.2 there are finitely many (up to $\simeq$) of those. Also $(A \times A^\vee)^4$ has finitely many direct factors (theorem 15.3). ∎

1.10 The Rosati involution (Alex)

Let A/k be an abelian variety and $f \in \mathrm{End}(A)$. Via pullback we get $\hat{f} \in \mathrm{End}(\hat{A})$, in the case where A is polarized i.e. we have an isogeny $\phi\colon A \to \hat{A}$ we might wonder what the relation is between $\hat{f}$ and f. E.g. $\hat{\mathrm{id}} = \mathrm{id}$ but here we have $\hat{\phi}\mathrm{id}\phi = [\deg \phi]$, this is a little ugly, depends on the degree of our polarization. If we work with $\mathrm{Hom}^0(A, B) = \mathrm{Hom}(A, B) \otimes \mathbf{Q}$ rather than $\mathrm{Hom}(A, B)$ we have a bona fide inverse ϕ^{-1} of an isogeny ϕ. So now we can ask precisely, what is the relationship of the endomorphism $f^\dagger = \phi^{-1} \circ \hat{f} \circ \phi \in \mathrm{End}^0(A)$ with f?

What sort of properties does this map $f \mapsto f^\dagger$ have?

Definition 1.10.1 The Rosati involution. The map $\phi^{-1}\hat{-}\phi = -^\dagger \colon \mathrm{End}^0(A) \to \mathrm{End}^0(A)$ is called the **Rosati involution**. ◊

Proposition 1.10.2 $-^\dagger$ *is* $\mathbf{Q}$*-linear*

Proposition 1.10.3 $-^\dagger$ *is an anti-homomorphism i.e.*

$$(fg)^\dagger = g^\dagger f^\dagger$$

Proposition 1.10.4 *Recall the l-adic Weil pairing for* $l \neq \mathrm{char}(k)$*, fix* $a, a' \in V_l A = T_l A \otimes \mathbf{Q}$*, then*

$$e_l^\phi(fa, a') = e_l^\phi(a, f^\dagger a').$$

Proof.

$$e_l^\phi(fa, a') = e_l(fa, \phi a') = e_l(a, \hat{f}\phi a') = e_l(a, \phi\phi^{-1}\hat{f}\phi a') = e_l^\phi(a, f^\dagger a') \quad \blacksquare$$

Proposition 1.10.5 $-^\dagger$ *is an involution, i.e.*

$$\alpha^{\dagger^\dagger} = \alpha.$$

Proof. We apply the previous proposition and skew-symmetry of a polarization (over some extension)

$$e_l^\lambda(\alpha a, a') = e_l^\lambda(a, \alpha^\dagger a') = e_l^\lambda(\alpha^{\dagger^\dagger} a, a')$$

for all $a, a' \in V_l A$. ■

So we have a weird algebra with a weird operation, what can we do? Perhaps inspired by the killing form of a lie algebra:

We can form a bilinear form using the trace

$$\mathrm{End}^0(A) \times \mathrm{End}^0(A) \to \mathbf{Q}$$

$$(f, g) \mapsto \mathrm{tr}(fg^\dagger).$$

Proposition 1.10.6 *This is positive definite. In fact*

$$\mathrm{tr}(ff^\dagger) = 2g\frac{(D^{g-1} \cdot f^*(D))}{(D^g)}$$

for $\phi = \phi_{\mathcal{L}(D)}$.

So given a simple abelian variety we have a division algebra $/\mathbf{Q}$ equipped with a positive definite involution.

Definition 1.10.7 Albert algebras? A division algebra D finite over $\mathbf{Q}$ with an involution $'$ such that $\mathrm{tr}_{D/\mathbf{Q}}(xx') > 0\ \forall x \in D^\times$ is called an **Albert algebra**. ◊

Such algebras were studied by Albert who proved an important classification theorem.

Theorem 1.10.8 Albert (1934/5). *Let* $(D, ')$ *be an Albert algebra, let* K *be the center of* D *and* K_0 *the subfield fixed by* $'$*. Then we have the following classification*

1. *Type I: $D = K = K_0$ a totally real number field and $'$ is the identity.*
2. *Type II: D is a quaternion algebra over $K = K_0$ a totally real field, that is split at all infinite places and $'$ is defined by letting starting with the standard quaternion algebra conjugation for which $x + x^* = \operatorname{tr}(x)$ and then letting $x' = ax^*a^{-1}$ for some $a \in D$ for which $a^2 \in K$ and is totally negative.*
3. *Type III: D is a quaternion algebra over $K = K_0$ a totally real field, that is ramified at all infinite places and $'$ is the standard quaternion algebra conjugation as above.*
4. *Type IV: D is a division algebra over a CM field K and K_0 is the maximal totally real subfield. Additionally if v is a finite place with $v = \bar{v}$ we have $\operatorname{Inv}_v(D) = 0$ and $\operatorname{Inv}_v(D) + \operatorname{Inv}_{\bar{v}}(D) = 0$ for all places v.*

There is a fascinating table in Mumford, page 200 or something.

As one might hope, changing the polarization does not change the type of the algebra + involution pair.

One might wonder which endomorphisms are invariant under this process? I.e. what is

$$\{f \in \operatorname{End}^0(A) : f^\dagger = f\}.$$

Equivalently, for which f is the dual given by conjugating by our polarization.

We can map

$$\mathbf{Q} \otimes_{\mathbf{Z}} \operatorname{NS}(X) = \mathbf{Q} \otimes_{\mathbf{Z}} \operatorname{Pic} X/\operatorname{Pic}^0 X \longrightarrow \operatorname{Hom}(A, \hat{A})$$

$$\mathcal{M} \mapsto \phi_{\mathcal{M}},$$

however we also have an isomorphism

$$\operatorname{Hom}^0(A, \hat{A}) \xrightarrow{\sim} \operatorname{End}^0(A)$$

$$\phi \mapsto \lambda^{-1}\phi$$

for some fixed polarization λ, hence we can view $\operatorname{NS}(A) \otimes \mathbf{Q}$ inside $\operatorname{End}^0(A)$.

Proposition 1.10.9 *Assume k algebraically closed. The image of*

$$\mathbf{Q} \otimes_{\mathbf{Z}} \operatorname{NS}(X) \longrightarrow \operatorname{End}^0(A)$$

is the fixed subspace

$$\{f \in \operatorname{End}^0(A) : f^\dagger = f\}.$$

Proof. Fix $\alpha \in \operatorname{End}^0(A)$ and $l \neq \operatorname{char}(k)$ odd. Applying Proposition 1.9.8 we see that $\lambda\alpha = \phi_{\mathcal{L}}$ for some $\mathcal{L}$ iff $e_l^{\lambda\alpha}$ is skew-symmetric, but we also have

$$e_l^{\lambda\alpha}(a, a') = e_l^{\lambda}(a, \alpha a') = -e_l^{\lambda}(\alpha a', a) = -e_l(a', \hat{\alpha}\lambda a)$$

for all $a, a' \in V_l A$ this is the same as requiring $\lambda\alpha = \hat{\alpha}\lambda$ i.e. $\alpha = \alpha^\dagger$. . ∎

Another cool result we can now prove (in fact this was the reason Weil introduced the notion of a polarization).

Theorem 1.10.10 *The automorphism group of a polarized abelian variety is finite.*

Proof. Let α be an automorphism of (A, λ) i.e. $\lambda = \hat{\alpha}\lambda\alpha$, then $\alpha^\dagger\alpha = 1$ and so

$$\alpha \in \operatorname{End}(A) \cap \{\beta \in \operatorname{End}(A) \otimes \mathbf{R} : \operatorname{Tr}(\alpha^\dagger\alpha) = 2g\}$$

but $\operatorname{End}(A)$ is discrete inside the compact RHS. ∎

1.11 Abelian Varieties over finite fields (Ricky)

Set $q = p^m$, p prime. Given $X/\mathbf{F}_q$ have geometric Frobenius $\pi_X\colon X \to X$ which acts as id on $|X|$ and sends $f \to f^q$ for $f \in \mathcal{O}_X(U)$.

Example 1.11.1 $X \hookrightarrow \mathbf{P}^n$ then $\pi_X(a_0 : \cdots : a_n) = (a_0^q : \cdots : a_n^q)$. □

We also have absolute Frobenius

$$F\colon X \to X^{(p)}.$$

Example 1.11.2

$$X\colon y^2 = x^3 + i/\mathbf{F}_q$$

$$X^{(p)}\colon y^2 = x^3 + i^3 = x^3 - i/\mathbf{F}_q$$

□

We see that $X^{(p^m)} = X$ and $F^m = \pi_X$.

$$\begin{tikzcd}
X \arrow[dr] \arrow[drr] \arrow[ddr] & & \\
& X^{(p)} \arrow[r] \arrow[d] & X \arrow[d] \\
& \mathbf{F}_q \arrow[r, "p"'] & \mathbf{F}_q
\end{tikzcd}$$

If $f\colon X \to Y$ of $\mathbf{F}_q$-schemes then $\pi_Y \circ f = f \circ \pi_X$. Now let X be an abelian variety over $\mathbf{F}_q$. From above, we have π_X commutes with all elements of $\operatorname{End}^0(X) = \operatorname{End}^0(X) \otimes \mathbf{Q}$. Let f_X be the characteristic polynomial of $T_l(\pi_X)\colon V_l(X) \to V_l(X)$ for $l \neq p$.

An alternative definition is to take $f_X \in \mathbf{Z}[X]$ monic of degree $2g$, $g = \dim X$ s.t.

$$f_X(n) = \deg([n] - \pi_X),$$

see 12.8.

Proposition 1.11.3 16.3. *Assume X is elementary, (i.e. its isogenous to A^n for some A simple). Then $\mathbf{Q}[\pi_X] \subseteq \operatorname{End}^0(X)$ is a field and f_X is a power of the minimal polynomial of π_X over $\mathbf{Q}$.*

Proof. Since X is elementary $Z(\operatorname{End}^0(X))$ is a field containing $\mathbf{Q}[\pi_X]$. Let g be the minimal polynomial of π_X over $\mathbf{Q}$. Let α be a root of f. Then $g(\alpha)$ is an eigenvalue of $g(V_l(\pi_X)) = V_l(g(\pi_X)) = V_l(0) = 0$. Hence $g(\alpha) = 0$. ■

Theorem 1.11.4 16.4. *Let $g = \dim(X)$.*

1. *Every root of f_X $\alpha \in \mathbf{C}$ satisfies $|\alpha| = q^{1/2}$.*

2. *If α is a root of f_X, then $\bar{\alpha}$ with the same multiplicity. In particular if $\alpha = \pm\sqrt{q}$ then it occurs with even multiplicity.*

We need some facts before proving this: Ref 5.20, 5.21

- There exists

  $$V\colon X^{(p)} \to X$$

  such that

  $$V \circ F = [p]_X$$

and

$$F \circ V = [p]_{X^{(p)}}.$$

Using $\deg F = p^g$ get $\deg V = p^g$

- By induction $[p^m] = V^m \circ F^m$.

We also need some facts about F and V relative to $X^\vee$.

$$F_X^\vee = V_{X^\vee} : (X^\vee)^{(p)} \longrightarrow X^\vee$$

identifying $(X^\vee)^{(p)} = (X^{(p)})^\vee$, Ref 7.33, 7.34.

Proof. Reduce to the case where X is simple, we have

$$h \colon X \longrightarrow X_1 \times X_2 \times \cdots \times X_s$$

an isogeny with X_i simple, then h induces an isomorphism

$$h \colon V_l(X) \xrightarrow{\sim} \bigoplus_i V_l(X_i)$$

so $f_X = f_{X_1} \cdots f_{X_s}$. Hence we can assume X is simple.

Let $\lambda \colon X \longrightarrow X^\vee$ be a polarization of X and $\dagger$ be the corresponding Rosati involution on $\mathrm{End}^0(X)$ we will show that $\pi_X \pi_X^\dagger = q$.

$$\pi_X \pi_X^\dagger = \pi_X \lambda^{-1} \pi_X^\vee \lambda = \lambda^{-1} \pi_{X^\vee} \pi_X^\vee \lambda = \lambda^{-1}[q]\lambda = [q]$$

To see $\pi_{X^\vee} = \pi_X^\vee = q$ we use $\pi_X = F^m$ and $\pi_X^\vee = V^m$. So $\pi_{X^\vee}\pi_X^\vee = F^M V^M = p^m = q$. As X is simple $\mathbf{Q}[\pi_X]$ is a field. Thus f_X is a power of g, the minimal polynomial of $\pi_X/\mathbf{Q}$. So the complex roots of f_X are $\iota(\pi_X)$ for every embedding $\mathbf{Q}[\pi_X] \hookrightarrow \mathbf{C}$. since $\pi_X^\dagger = q/\pi_X$, we see that

$$\mathbf{Q}[\pi_X] \subseteq \mathrm{End}^0(X)$$

is stable under $\dagger$. We have two cases for such a $K = \mathbf{Q}[\pi_X]$

1. K is totally real and $\dagger = \mathrm{id}$.
2. K is a CM field and $\dagger = \bar{\cdot}$.

hence we get

$$\iota(\pi_X \pi_X^\dagger) = \iota(\pi_X)\overline{\iota(\pi_X)} = q$$

for any $\iota \colon K \longrightarrow \mathbf{C}$.

If $\pm\sqrt{q}$ is a root of f_X then we are in the case of K totally real. If $\sqrt{q}$ has multiplicity n. Then $-\sqrt{q}$ has multiplicity $2g - n$. Thus $f_X(0) = (-1)^n q^g$. But also $f_X(0) = \deg(0 - \pi_X) = q^g$. Hence n is even. ∎

Honda-Tate. The correspondence between isogeny classes of $X/\mathbf{F}_q$ and conjugacy classes of q-Weil numbers is a bijection. (i.e. algebraic integers α s.t. $|\iota\alpha| = \sqrt{q}$ for all $\iota \colon \mathbf{Q}(\alpha) \hookrightarrow \mathbf{C}$).

Using relations between a curve $C/\mathbf{F}_q$ and its Jacobian $J(C)$, one can show:

Theorem 1.11.5 Hasse-Weil-Serre bound.

$$q + 1 - g\lfloor 2\sqrt{q} \rfloor \leq \#C(\mathbf{F}_q) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor$$

where $g = g(C)$.

Proof. Hint: Use Lefschetz trace and $H^1(C, \mathbf{Q}_l) \simeq H^1(J(C), \mathbf{Q}_l)$. ∎

Application: Let $J = J_0(103) = J(X_0(103))$. $J \sim J_+ \times J_-$.

$$J_\pm = \mathrm{im}(w \pm \mathrm{id})$$

w Atkin-Lehner. $\dim J = 8$ and $\dim(J_-) = 6$. In fact $\exists f \in S_2(\Gamma_0(103))$ an eigenform s.t. if

$$f = \sum_{n\geq 1} a_n q^n$$

then $[\mathbf{Q}(a_n)_{n\geq 1} : \mathbf{Q}] = 6$ and $\mathrm{tr}(F_{J_-,p}; T_l(J_-)) = \mathrm{tr}_{K/\mathbf{Q}}(a_p)$ for $l \neq p, p \neq 103$ We can compute $\mathrm{tr}_{K/\mathbf{Q}}(a_2) = 4$. This implies that $J_- \times \mathbf{F}_2$ is not the Jacobian of a curve $/\mathbf{F}_2$, if it were, then if $J_- \times \mathbf{F}_2 = J(C)$ then via Lefschetz trace formula

$$\#\mathrm{C}(\mathbf{F}_2) = 2 + 1 - 4 = -1$$

similar thing at 17.

1.12 Tate's Isogeny Theorem (Sachi)

1.12.1 The Theorem

Theorem 1.12.1 Tate. *Let $A, B/\mathbf{F}_q = k$, $q = p^n$, $l \neq p$ be abelian varieties and $G = \mathrm{Gal}(k^s/k)$, then*

$$\mathrm{Hom}_k(A, B) \otimes \mathbf{Z}_l \to \mathrm{Hom}_G(T_l A, T_l B) = \mathrm{Hom}_{\mathbf{Z}_l}(T_l A, T_l B)^G$$

(where the G action on $\mathrm{Hom}_{\mathbf{Z}_l}(T_l A, T_l B)$ is $(gf)(x) = gf(g^{-1}x)$) is an isomorphism.

Remark 1.12.2 Tate's theorem is also true for function fields over finite fields (Zarhin) and fields that are finitely generated over their prime field (Faltings), e.g. number fields. Not true over algebraically closed fields though.

1.12.2 Motivation

Let π_A and π_B be the (relative) Frobenii on $V_l(A), V_l(B)$

$$\mathrm{Hom}_k(A, B) \otimes \mathbf{Q}_l \to \mathrm{Hom}_G(V_l A, V_l B)$$

P_A, P_B characteristic polynomials of π_A, π_B.

Toy Weil conjectures: P_A, P_B have $\mathbf{Z}$-coefficients, don't depend on the choice of l. Provided that induced action of Frobenii are semisimple, we can find a number $r(P_A, P_B)$ then Tate implies

$$r(P_A, P_B) = \dim_{\mathbf{Q}_l} \mathrm{Hom}_G(V_l(A), V_l(B)) = \mathrm{rank}\, \mathrm{Hom}_k(A, B)$$

Corollary 1.12.3 *Let A, B be abelian varieties over $\mathbf{F}_q$ and P_A, P_B as above*

1. $$\mathrm{rank}\, \mathrm{Hom}_k(A, B) = r(P_A, P_B)$$

2. *TFAE*

   (a) *B is k-isogenous to an abelian subvariety of A*

   (b) *$V_l B$ is G-isomorphic to a G-subrepresentation of $V_l A$ for $l \neq \mathrm{char}\, k$*

   (c) $$P_B | P_A$$

we also have similar statements for equivalence, but get a nice statement about counting points over all extensions determining an abelian variety.

Proof.

$$\alpha\colon V_l(B) \hookrightarrow V_l(A)$$

the surjectivity in Tate's theorem means we can choose $u \in \mathrm{Hom}_k(B,A) \otimes \mathbf{Q}_l$. $V_l(u) = \alpha$. Choose $u \in \mathrm{Hom}_k(B,A) \otimes \mathbf{Q}$ arbitrarily close to α. Lower semicontinuity implies if $V_l(u)$ is close enough to α, can ensure $V_l(u)$ is injective ($\ker(V_l(u)) = 0$) take multiple to get $u \in \mathrm{Hom}_k(B,A)$. Since $T_l(u)$ is injective u is an isogeny to an abelian subvariety. ∎

1.12.3 Isogeny category

Recall: The isogeny category, Theorem 1.7.1, Corollary 1.7.3. So we have a category $\mathcal{I}\mathfrak{f}\}$ of abelian varieties with

$$\mathrm{Hom}_{\mathcal{I}\mathfrak{f}\}}(A,B) = \mathrm{Hom}_{\mathcal{AV}}(A,B) \otimes \mathbf{Q}.$$

Now if $f\colon A \to B$ there exists $g\colon B \to A$ an isogeny and $n \in \mathbf{Z}_{\geq 1}$ s.t. $gf = [n]$. So $\frac{1}{n}g$ is an inverse for $f \in \mathcal{I}\mathfrak{f}\}$ so isogenies are isomorphisms in $\mathcal{I}\mathfrak{f}\}$.

$\mathcal{I}\mathfrak{f}\}$ is a semisimple abelian category. The simples are simple abelian varieties.

1. Decomposition up to isogeny into a product of simple abelian varieties is unique.

2. If A is simple $\mathrm{End}\,A \otimes \mathbf{Q}$ is a division algebra over $\mathbf{Q}$. Reason: If A is simple in an abelian category, if $\mathrm{End}\,A \supseteq k$ a field implies it's a division algebra.

1.12.4 Reductions

Lemma 1.12.4

1.
$$\mathbf{Z}_l \otimes \mathrm{Hom}_{\mathcal{AV}}(A,B) \to \mathrm{Hom}_H(T_l, T_l B)$$
is an isomorphism if and only if
$$\mathbf{Q}_l \otimes \mathrm{Hom}_{\mathcal{AV}}(A,B) \to \mathrm{Hom}_G(V_l A, V_l B)$$
is an iso

2. *If for every C,*
$$\mathbf{Q}_l \otimes \mathrm{End}_{\mathcal{AV}}(C) \to \mathrm{End}_G(V_l C)$$
is an isomorphism then the above is an isomorphism for every pair A,B.

Proof.

1. The first map is always injective, the cokernel is torsion free, hence free. It's an isomorphism if and only if $\mathbf{Q}_l \otimes \mathrm{coker} = 0$ As $\mathbf{Q}_l$ is flat over $\mathbf{Z}_l$ the second map injective and its cokernel is $\mathbf{Q}_l \otimes$ the cokernel of the first map.

2.
$$C = A \times B$$

then

$$\mathrm{End}^0(C) = \mathrm{End}^0(A) \oplus \mathrm{Hom}^0(A, B) \oplus \mathrm{Hom}^0(B, A) \oplus \mathrm{End}^0(B)$$

and

$$\mathrm{End}_G(V_l C) = \mathrm{End}_G(V_l A) \oplus \mathrm{Hom}_G(V_l A, V_l B) \oplus \mathrm{Hom}_G(V_l B, V_l A) \oplus \mathrm{End}_G(V_l B)$$

which the injection above preserves, in particular if the last map is an isomorphism, so are the rest.

■

One more reduction!

$$E_l = \mathrm{End}_k(A) \otimes \mathbf{Q}_l \subseteq \mathrm{End}_{\mathbf{Q}_l}(V_l A)$$

$$F_l = \mathbf{Q}_l[G] \subseteq \mathrm{End}_{\mathbf{Q}_l}(V_l A)$$

automorphisms of $V_l(A)$ coming from G.

Note 1.12.5 E_l coming from k-rational endomorphisms commute with the Galois action

$$F_l \subseteq C_{\mathrm{End}_{\mathbf{Q}_l}(V_l(A))}(E_l)$$

want equality.

Lemma 1.12.6

1. *The last map of the reduction lemma is an isomorphism if and only if*

$$C(C(E_l)) = \mathrm{End}_G(V_l(A))$$

2. *If F_l is semisimple the map is an isomorphism if and only if*

$$C(E_l) = F_l$$

Proof.

1. Double centralizer theorem, if E_l is semisimple then $C(C(E_l)) = E_l$. Poincaré reducibility implies

$$A \sim \prod A_i^{m_i}$$

$$\mathrm{End}^0(A) = \mathrm{End}^0(\prod A_i^{m_i}) = \prod \mathrm{Mat}_{m_i}(\mathrm{End}^0(A_i))$$

a finite dimensional division algebra $/\mathbf{Q}$. A matrix algebra over a finite dimensional division algebra is semisimple.

2. If F_l is semisimple

$$C(E_l) = F_l \iff E_l = C(C(E_l))$$

so

$$E_l = C(F_l) = \mathrm{End}_G(V_l(A)).$$ ■

1.12.5 Proof of Tate using finiteness

We introduce a hypothesis: $\mathrm{Hyp}(k, A, l)$ there exist only finitely many (up to k-isomorphism) abelian varieties B s.t. there is a k-isogeny of l-power degree from $B \to A$.

$D = C(E_l)$ want that $C(D) = \mathrm{End}_G(V_l(A))$ know $C(D) \subseteq E_l \subseteq \mathrm{End}_G(V_l(A))$ want $C(D) \supseteq \mathrm{End}_G(V_l(A))$. Let $\alpha \in \mathrm{End}_G(V_l(A))$ show that it commutes with everything in D. Equivalently let W be the graph of α

$$W = \{(x, \alpha x) \in V_l(A) \times V_l(A)\} \subseteq V_l(A) \times V_l(A)$$

note $g \in G$ then $g \circlearrowright (x, \alpha x) = (gx, g\alpha x) = (gx, \alpha(gx))$.

$$\alpha \in C(D) \iff \forall x \in V_l(A), d \in D$$

$$\alpha dx = d\alpha x \iff (d \oplus d)W \subseteq W \forall d \in D$$

$$W \ni (dx, d\alpha x) = (dx, \alpha dx)$$

Lemma 1.12.7 Technical lemma. *If $W \subseteq V_l(A)$ is G-stable subspace then there exists $u \in E_l$ s.t. $uV_l(A) = W$.*

Proof. For $n \in \mathbf{Z}_{\geq 0}$ let $U_n = (W \cap T_l(A)) + l^n T_A$ which is a G-stable lattice in $V_l A$,

$$l^n T_l A \subseteq U_n \subseteq T_l A$$

let $\mathcal{K}_n \subseteq A[l^n](k^s) = T_l A / l^n T_l A$ be the image of U_n. $\mathcal{K}_n$ is stable under G-action on $A[l^n](k^s)$ which implies $\mathcal{K}_n = K_n(k^s)$. Let $\pi_n \colon A \to B_n = A/K_n$, $\iota_n \colon B_n \to A$ unique isogeny s.t.

$$\iota_n \circ \pi_n = [[l^n]_A$$

then $T_l B \cong U_n$ as $\mathbf{Z}_l$-modules with G-action. As $T_l(\iota_n)\colon U_n = T_l B \to T_l A$ is the inclusion map. Assuming $\mathrm{Hyp}(k, A, l)$ we can find $n = n_1 < n_2 < \cdots$ s.t. we have

$$\alpha_i \colon B_n \xrightarrow{\sim} B_{n_i}$$

$$\begin{tikzcd} B_n \arrow[r, "\alpha_i"] & B_{n_i} \arrow[d, "\iota_{n_i}"] \\ A \arrow[u, "\pi_n"] \arrow[r, dashed, "u_i"'] & A \end{tikzcd}$$

$u_i = \iota_{n_i} \circ \alpha_i \circ \pi_n$ is an endomorphism of A on Tate modules $T_l(u_i)$ is induced map

$$T_l A \xrightarrow{[l^n]} U_n \xrightarrow{T_l \alpha_i} U_{n_i} \hookrightarrow T_l A$$

because $\mathbf{Z}_l \otimes \mathrm{End}\, A$ is a free $\mathbf{Z}_l$-module of finite rank compact in l-adic topology subsequence of $u_i \to u$ in $\mathbf{Z}_l \otimes \mathrm{End}\, A$

$$U_{n_1} \supseteq U_{n_2} \supseteq \cdots$$

the endomorphism of $T_l u$ maps $T_l A$ to $\bigcap_{i=1}^{\infty} U_{n_i} = W \cap T_l A$ passing to $\mathbf{Q}_l$-coefficients, note $\mathbf{Q}_l(W \cap T_l A) = \mathbf{Q}_l(l^n(W \cap T_l A)) = W$ so $\mathrm{im}(V_l(u)) = W$. ∎

Why does the hypothesis hold.

Fact 1.12.8 *There exists a moduli space of d-polarised abelian varieties of* $\dim = g$ *$A_{g,d}$ which is a stack of finite type $/k$.*

$$A_{g,d}(k) = \{(A, \lambda) : A, \lambda \colon A \to A^\vee,\ \deg d\}$$

Zahrin's trick: A abelian variety $(A \times A^\vee)^4$ is principally polarized. Finiteness of direct factors $B \subseteq A$ $A \simeq B \times C$.

Corollary 1.12.9 *If $k = \mathbf{F}_q$ exists only finitely many isogeny classes of abelian varieties of* dim g.

Proof. A is a direct factor $(A \times A^\vee)^4 \in A_{8g,1}$. ∎

Proof. of Tate.
Apply technical lemma to $V_l(A \times A)$ and W so

$$(d \oplus d)W = (d \oplus d)uV_l(A \times A) = u(d \oplus d)V_l(A \times A) \subseteq uV_l(A \times A) = W$$

$$\implies C(D) \supseteq \mathrm{End}_G(V_l(A)).$$ ∎

1.13 The Honda Tate Theorem (Angus)

$q = p^n$, A a simple abelian variety over $\mathbf{F}_q$, π_A the frobenius on A, $\mathrm{End}^0(A) = \mathbf{Q} \otimes \mathrm{End}(A)$, f_A is the charpoly of A (i.e. of π_A).

Fact 1.13.1

- $\mathrm{End}^0(A)$ *is a division ring.*
- $\mathbf{Q}[\pi]$ *is a field.*
- $Z(\mathrm{End}^0(A)) = \mathbf{Q}[\pi_A]$

Lemma 1.13.2 The Weil Conjectures. *The roots of f_A all have absolute value $\sqrt{q}$. Alternatively, under all embeddings*

$$\iota\colon \mathbf{Q}[\pi_A] \hookrightarrow \mathbf{C},\ |\iota(\pi_A)| = \sqrt{q}.$$

Definition 1.13.3 q-Weil numbers. A **q-Weil number** is an algebraic integer π s.t.

$$\forall \iota\colon \mathbf{Q}[\pi] \hookrightarrow \mathbf{C},\ |\iota(\pi)| = \sqrt{q}$$

we say that two q-Weil numbers are conjugate if they have the same minimal polynomial over $\mathbf{Q}$, and write $\pi \sim \pi'$. ◊

From the facts so far we have a map

$$\{\text{simple AVs}/\mathbf{F}_q\} \longrightarrow \{q\text{-Weil numbers}\}$$

$$A \longmapsto \pi_A$$

Theorem 1.13.4 *We have a bijection*

$$\{\textit{isogeny classes of simple AVs}/\mathbf{F}_q\} \xrightarrow{\sim} \{\textit{conjugacy classes of } q\textit{-Weil numbers}\}$$

$$A \longmapsto \pi_A.$$

We need to show this is well-defined, injectivity and surjectivity.

1.13.1 Honda-Tate map

Recall:

Corollary 1.13.5 *Let A, B be abelian varieties over $\mathbf{F}_q$ with rational Tate modules V_lA, V_lB then*

$$A \sim_{isog} B \iff V_lA \simeq V_lB \forall l \neq p.$$

Corollary 1.13.6

$$A \sim_{isog} B \iff f_A = f_B$$

Proof. By above $V_l A \simeq V_l B$ for all $l \neq p$ but f_A (resp. f_B) is the charpoly of π_a (π_B) on $V_l A$ ($V_l(B)$).

The Galois modules $V_l A$ and $V_l B$ are semisimple. The Brauer-Nesbitt theorem says $f_A = f_B \implies V_l A \simeq V_l B$ for $l \neq p$. ∎

Recalling that f_A is a power of the minimal polynomial of π_A,

$$A \sim_{\text{isog}} B \implies f_A = f_B \implies \pi_A \sim \pi_B.$$

So the Honda-Tate map is well defined.

This doesn't quite give injectivity because a priori f_A and f_B could be powers of the minpolys of π_A, π_B.

1.13.2 Injectivity and Brauer groups

From last time:

Proposition 1.13.7 *There exists a certain quantity $r(f_A, f_B)$ such that*

$$r(f_A, f_B) = \operatorname{rank}\operatorname{Hom}(A, B).$$

Corollary 1.13.8 *Let $d = [\operatorname{End}^0(A) : \mathbf{Q}(\pi_A)]^{1/2}$, let $h_A = \operatorname{minpoly}_{\mathbf{Q}}(\pi_A)$ then $f_A = h_A^d$.*

Proof. Study the formula for $r(f_A, f_A)$ Edixhoven-van der Geer-Moonen 16.22. ∎

So the next step is to try and recover $\operatorname{End}^0(A)$ from π.

Definition 1.13.9 Central simple algebras. A **central** simple **algebra** B/k is a k-algebra B with no two-sided ideals and $Z(B) = k$. ◊

Theorem 1.13.10 Artin-Wedderburn. *Any such algebra is isomorphic to $M_n(D)$ for D a division ring over k.*

Definition 1.13.11 Brauer groups. The **Brauer group** of k $\operatorname{Br}(k)$ is the set of central simple algebras under $\otimes$ modulo the algebras $M_n(k)$. ◊

Fact 1.13.12

- *If $k = \overline{k}$,* $\operatorname{Br}(k) = 0$.
- *k complete nonarchimidean* $\operatorname{Br}(k) = \mathbf{Q}/\mathbf{Z}$
- $\operatorname{Br}(\mathbf{R}) = \mathbf{Z}/2\mathbf{Z}$

Given a place v of k we get a map

$$\operatorname{Br}(k) \longrightarrow \operatorname{Br}(k_v)$$
$$D \mapsto D \otimes k_v$$

in fact we get an injection

$$\operatorname{Br}(k) \hookrightarrow \prod_v \operatorname{Br}(k_v) \simeq \prod_{v \text{ nonarch}} \mathbf{Q}/\mathbf{Z} \times \prod_{v \text{ real}} \mathbf{Z}/2\mathbf{Z}$$
$$D \mapsto (\operatorname{inv}_v(D))_v$$

these $\operatorname{inv}_v(D)$ *are called the* ***local invariants***.

Proposition 1.13.13 *Let $A/\mathbf{F}_q$ be an elementary abelian variety. Let $K = \mathbf{Q}(\pi_A)$ then*

$$\mathrm{inv}_v(\mathrm{End}^0(A)) = \begin{cases} \frac{v(\pi_A)}{v(q)}[k_v : \mathbf{Q}_p], & v|p \\ \frac{1}{2}, & v \text{ real} \\ 0, & \text{else} \end{cases}$$

Proof. Edixhoven-van der Geer-Moonen 16.30. ∎

Proposition 1.13.14 *Let $d = [\mathrm{End}^0(A) : \mathbf{Q}(\pi_A)]^{1/2}$ then d is the least common denominator of all the* $\mathrm{inv}_v(\mathrm{End}^0(A))$.

Corollary 1.13.15

$$\pi_A \sim \pi_B \iff f_A = f_B.$$

Proof. $\Leftarrow$ done.

$\Rightarrow$ Let D_{π_A}, D_{π_B} be the division rings with invariants specified as in Proposition 1.13.13. $\pi_A \sim \pi_B \implies D_{\pi_A} \simeq D_{\pi_B} \implies f_A = \mathrm{minpoly}(\pi_A)^d = f_B$. ∎

1.13.3 Surjectivity and CM theory

We need to show that for π a q-Weil number there exists an abelian variety $A/\mathbf{F}_q$ such that $\pi_A \sim \pi$.

Definition 1.13.16 Such a q-Weil number π is called effective. ◊

Proposition 1.13.17 *A q-Weil number π is effective if and only if π^N is effective for some $N \in \mathbf{Z}_{\geq 1}$.*

Proof. $\Rightarrow$ clear.

$\Leftarrow$ By assumption we have A'/k a simple abelian variety s.t. $\pi_{A'} \sim \pi^N$ for k a degree N extension of $\mathbf{F}_q$. Let

$$A = \mathrm{Res}_{k/\mathbf{F}_q}(A')$$

on the rational Tate modules we have

$$V_l A = \mathrm{Ind}_{G_k}^{G_{\mathbf{F}_q}}(V_l A')$$

where

$$G_k = \mathrm{Gal}(\overline{\mathbf{F}_q}/k)$$

$$G_{\mathbf{F}_q} = \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$$

since $G_k, G_{\mathbf{F}_q}$ are abelian, by studying the induced action, one can see

$$\mathrm{Ind}_{G_k}^{G_{\mathbf{F}_q}}(\pi_{A'}) = \pi_A^N$$

in particular $f_A(T) = f_{A'}(T^N)$. Choosing a simple factor A_i one gets $\pi_{A_i} \sim \pi$. ∎

So it is sufficient to show π^N is effective.
Strategy for proving surjectivity

1. Construct a division algebra D_π.
2. Choose a CM field L splitting D_π.

3. Find an abelian variety $A/\mathbf{C}$ of type (L, Φ).
4. In fact A is defined over a number field K and has good reduction at $v|p$.
5. Apply the Shimura-Taniyama formula to relate π_A to Φ.
6. Choose Φ wisely (in retrospect in 3) to relate π to π_A.
7. Show $\pi_A^N = \pi^{N'}$.

D_π is given by the invariants described by π (and $K = \mathbf{Q}(\pi)$).

Proposition 1.13.18 *There exists a CM field $L/\mathbf{Q}(\pi)$ such that L splits D_π and further*

$$[L : \mathbf{Q}(\pi)] = [D_\pi : \mathbf{Q}(\pi)]^{1/2}$$

Proof. Two cases:

1. $\mathbf{Q}(\pi)$ is totally real, in which case $\mathbf{Q}(\pi) = \mathbf{Q}$ or $\mathbf{Q}(\sqrt{p})$.
2. $\mathbf{Q}(\pi)$ is a CM field with totally real subfield $\mathbf{Q}(\pi + q/\pi)$.

In the case

1. Choose $L = \mathbf{Q}(\pi)(\sqrt{-p})$.
2. Let $d = [D_\pi : \mathbf{Q}(\pi)]^{1/2}$. This L splits D_π.

■

Definition 1.13.19 CM types. For a CM field L all the embeddings

$$\iota \colon L \hookrightarrow \mathbf{C}$$

come in complex conjugate pairs, choosing an embedding for each pair defines a subset $\Phi \subseteq \mathrm{Hom}(L, \mathbf{C})$ such that

$$\Phi \cup \overline{\Phi} = \mathrm{Hom}(L, \mathbf{C})$$

$$\Phi \cap \overline{\Phi} = \emptyset$$

such a choice of Φ is called a **CM type**. ◊

Let $A/\mathbf{C}$ be an abelian variety with CM by L i.e.

$$L \hookrightarrow \mathrm{End}^0(A)$$

then

$$\mathbf{C} \otimes L = \prod_\iota \mathbf{C}$$

acts on the tangent space at the origin $\mathrm{Lie}(A)$.

Proposition 1.13.20 *The action of $\mathbf{C} \otimes L$ factors through the quotient $\prod_{\iota \in \Phi} \mathbf{C}$ for some CM type Φ. We then say $A/\mathbf{C}$ is of type (L, Φ).*

Theorem 1.13.21 *For any CM type (L, Φ) there exists an abelian variety $A/\mathbf{C}$ of type (L, Φ).*

Proof. Found in Shimura-Taniyama. ■

The fact that A is in fact defined over a number field K is also in Shimura-Taniyama.

Theorem 1.13.22 *Let A/K be an abelian variety which admits CM. Then A/K admits potentially good reduction at all places v of K.*

Proof. Highly nontrivial, Neron models, Chevalley decomposition, Neron-Ogg-Shafarevich criterion, result of Grothendieck on potentially stable reduction. ∎

After passing to a finite extension we will assume A/K has good reduction at places $v|p$. So we have a reduction $A_{\mathbf{F}_{q'}}/\mathbf{F}_{q'}$. For a place $w|p$ of L let

$$\Sigma_w = \operatorname{Hom}(L_w, \mathbf{C}_p)$$

$$\Phi_w = \Phi \cap \Sigma_w.$$

Theorem 1.13.23 Shimura-Taniyama formula. *For all places $w|p$ of L,*

$$\frac{w(\pi_{A_{\mathbf{F}_{q'}}})}{w(q')} = \frac{\#\Phi_w}{\#\Sigma_w}$$

Proof. Tate has a proof using CM theory of p-divisible groups. ∎

Recall we fixed π and from this we deterministically formed $\mathbf{Q}(\pi), D_\pi, L$ however we have no restriction on our choice of Φ.

Lemma 1.13.24 *We can choose Φ such that for all places $w|p$ of L,*

$$\frac{w(\pi)}{w(q)} = \frac{\#\Phi_w}{\#\Sigma_w}$$

Proof. Let $v = w|_{\mathbf{Q}(\pi)}$ be the place of $\mathbf{Q}(\pi)$ below w. Let

$$n_w = \frac{w(\pi)}{w(q)}\#\Sigma_w = \frac{w(\pi)}{w(q)}[L_w : \mathbf{Q}_p]$$

$$= \frac{w(\pi)}{w(q)}[L_w : \mathbf{Q}(\pi)_v][\mathbf{Q}(\pi)_v : \mathbf{Q}_p]$$

by recalling the formula for the local invariants of D_π we get

$$n_w = \operatorname{inv}_w(D_\pi \otimes_{\mathbf{Q}(\pi)} L).$$

But L splits D_π so $n_w \in \mathbf{Z}$, further

$$n_w + n_{\overline{w}} = \left(\frac{w(\pi)}{w(q)} + \frac{\overline{w}(\pi)}{\overline{w}(q)}\right)\#\Sigma_w$$

$$= \left(\frac{w(\pi\overline{\pi})}{w(q)}\right)\#\Sigma_w = \#\Sigma_w$$

check the CM type $\Phi = \bigcup_w \Phi_w$ where for each w $\#\Phi_w = n_w$. Then the formula follows. ∎

Combining the previous result with the Shimura-Taniyama formula we get that for all places $w|p$

$$\frac{w(\pi_{A_{\mathbf{F}_{q'}}})}{w(q')} = \frac{w(\pi)}{w(q)}.$$

Taking the correct power,

$$w\left(\frac{\pi^m_{A_{\mathbf{F}_{q'}}}}{\pi^{m'}}\right) = 0 \forall w | p$$

$$\pi, \pi_{A_{\mathbf{F}_{q'}}} | q^{m'}$$

$$\implies w(\cdots) = 0 \forall w \nmid p$$

since $|\pi^{m'}|_w = |\pi^m_{A_{\mathbf{F}_{q'}}}|_w = (q^{m'})^{1/2} \forall$ infinite places

$$\pi_{A_{\mathbf{F}_{q'}}} / \pi_A^{m'}$$

is a root of unity $\pi^N_{A_{\mathbf{F}_{q'}}} = \pi^{N'}$.

Chapter 2

Dessins d'Enfants

These are notes for BUNTES Spring 2018, the topic is Dessins d'Enfants, they were last updated November 19, 2018. For more details see the webpage. These notes are by Alex, feel free to email me at `alex.j.best@gmail.com` to report typos/suggest improvements, I'll be forever grateful.

2.1 Overview (Angus)

2.1.1 Belyi morphisms

Let X be an algebraic curve over $\mathbf{C}$ (i.e. a compact Riemann surface) when is X defined over $\overline{\mathbf{Q}}$?

Theorem 2.1.1 Belyi. *An algebraic curve $X/\mathbf{C}$ is defined over $\overline{\mathbf{Q}}$ $\iff$ there exists a morphism $\beta\colon X \to \mathbf{P}^1\,\mathbf{C}$ ramified only over $\{0, 1, \infty\}$.*

Definition 2.1.2 Ramified. (AG) A morphism $f\colon X \to Y$ is **ramified** at $x \in X$ if on local rings the induced map $f^\#\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ descended to

$$\mathcal{O}_{Y,f(x)}/\mathfrak{m} \to \mathcal{O}_{X,x}/f^\#(\mathfrak{m})$$

is not a finite inseparable field extension.
(RS) A morphism $f\colon X \to Y$ is ramified at $x \in X$ if there are charts around x and $f(x)$ such that $f(x) = x^n$. This n is the **ramification index**. ◊

Definition 2.1.3 Belyi morphisms. A **Belyi morphism** is one ramified only over $\{0, 1, \infty\}$
A **clean Belyi morphism** or **pure Belyi morphism** is a Belyi morphism where the ramification indices over 1 are all exactly 2. ◊

Lemma 2.1.4 *A curve X admits a Belyi morphism iff it admits a clean Belyi morphism.*

Proof. If $\alpha\colon X \to \mathbf{P}^1\,\mathbf{C}$ is Belyi, then $\beta = 4\alpha(1-\alpha)$ is a clean Belyi morphism. ■

2.1.2 Dessin d'Enfants

Definition 2.1.5 A **dessin d'Enfant** (or Grothendieck Dessin or just **Dessin**) is a triple (X_0, X_1, X_2) where X_2 is a compact Riemann surface, X_1 is a graph, $X_0 \subset X_1$ is a finite set of points, where $X_2 \setminus X_1$ is a collection of open cells. $X_1 \setminus X_0$ is a disjoint union of line segments ◊

Lemma 2.1.6 *The data of a dessin is equivalent to a graph with an ordering on the edges coming out of each vertex.*

Definition 2.1.7 Clean dessins. A **clean dessin** is a dessin with a colouring (white and black) on the vertices such that adjacent vertices do not share a colour. ◊

2.1.3 The Grothendieck correspondence

Given a Belyi morphism $\beta\colon X \to \mathbf{P}^1\,\mathbf{C}$ the graph $\beta^{-1}([0,1])$ defines a dessin.

Theorem 2.1.8 *The map*

$$\{\text{(Clean) Belyi morphisms}\} \longrightarrow \{\text{(clean) dessins}\}$$

$$\beta \mapsto \beta^{-1}([0,1])$$

is a bijection up to isomorphisms.

Example 2.1.9

$$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C}$$

$$x \mapsto x^3$$

$$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C}$$

$$x \mapsto x^3 + 1$$

□

2.1.4 Covering spaces and Galois groups

A Belyi morphism defines a covering map.

$$\tilde{\beta}\colon \tilde{X} \to \mathbf{P}^1\,\mathbf{C} \setminus \{0, 1, \infty\}$$

the coverings are controlled by the profinite completion of

$$\pi_1(\mathbf{P}^1\,\mathbf{C} \setminus \{0,1,\infty\}) = \mathbf{Z} * \mathbf{Z} = F_2.$$

Theorem 2.1.10 *There is a faithful action*

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \circlearrowright \hat{\pi}_1(\mathbf{P}^1\,\mathbf{C} \setminus \{0,1,\infty\})$$

Proof. By Belyi's theorem every elliptic curve $E/\overline{\mathbf{Q}}$ admits a Belyi morphism. For each $j \in \overline{\mathbf{Q}}$ there exists an elliptic curve $E_j/\overline{\mathbf{Q}}$ with j-invariant j.

Given $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$,

$$\sigma(E_j) = E(\sigma(j))$$

assume $\sigma \mapsto 1$,

$$E_j \cong E_{\sigma(j)}\ \forall j$$

$$j = \sigma(j)\ \forall j$$

a contradiction. ■

Corollary 2.1.11 *We have a faithful action of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *on dessins.*

Theorem 2.1.12 *We have a faithful action of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *on the set of dessins of any fixed genus.*

2.1.5 Exercises

Exercise 2.1.13 Compute the Dessins for the following Belyi morphisms

1. $$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C},\ x \mapsto x^4$$

2. $$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C},\ x \mapsto x^2(3-2x)$$

3. $$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C},\ x \mapsto \frac{1}{x(2-x)}$$

Exercise 2.1.14 Give an alternate proof of the fact that X admits a Belyi morphism if and only if it admits a clean Belyi morphism using dessins and the Grothendieck correspondence.

Exercise 2.1.15 Prove that a Belyi morphism corresponding to a tree, that sends ∞ to ∞ is a polynomial.

2.2 Riemann Surfaces I (Ricky)

2.2.1 Definitions

Definition 2.2.1 A **topological surface** is a Hausdorff space X wich has a collection of charts

$$\{\phi_i : U_i \xrightarrow{\sim} \phi_i(U_i) \subseteq \mathbf{C},\ \text{open}\}_{i\in I}$$

such that

$$X = \bigcup_{i\in I} U_i.$$

We call X a **Riemann surface** if the transition functions $\phi_i \circ \phi_j^{-1}$ are holomorphic. ◊

2.2.2 Examples

Example 2.2.2 Open subsets of $\mathbf{C}$, e.g.

$$\mathbf{C}$$

$$\mathbf{D} = \{z \in \mathbf{C} : |z| < 1\}$$

$$\mathbf{H} = \{z \in \mathbf{C} : \operatorname{im} z > 0\}.$$

□

Example 2.2.3 $\hat{\mathbf{C}}$ = Riemann sphere = $\mathbf{C} \cup \{\infty\}$. A basis of neighborhoods of ∞ is given by

$$\{z \in \mathbf{C} : |z| > R\} \cup \{\infty\}.$$

□

Example 2.2.4

$$\mathbf{P}^1(\mathbf{C}) = \{[z_0 : z_1] : (z_0, z_1) \neq (0,0)\}$$
$$U_0 = \{[z_0, z_1] : z_0 \neq 0\} \to \mathbf{C}$$
$$[z_0 : z_1] \mapsto \frac{z_1}{z_0}$$
$$U_1 = \{[z_0, z_1] : z_1 \neq 0\} \to \mathbf{C}$$
$$[z_0 : z_1] \mapsto \frac{z_0}{z_1}.$$

□

Example 2.2.5 Let $\Lambda = \mathbf{Z} \oplus \mathbf{Z}i \subseteq \mathbf{C}$ then $X = \mathbf{C}/\Lambda$ is a Riemann surface. □

2.2.3 Morphisms

Definition 2.2.6 (Holo/Mero)-morphisms of Riemann surfaces. A **morphism of Riemann surfaces** is a continuous map

$$f : S \to S'$$

such that for all charts ϕ, ψ on S, S' respectively we have $\psi \circ f \circ \phi^{-1}$ is holomorphic.
We call a morphism $f : S \to \mathbf{C}$ a **holomorphic function** on S.
We say $f : S \to \mathbf{C}$ is a **meromorphic function** is $f \circ \phi^{-1}$ is meromorphic. ◊

Exercise 2.2.7 The set of meromorphic functions on a Riemann surface form a field.

We denote the field of meromorphic functions by $\mathcal{M}(S)$.

Proposition 2.2.8 1.26.

$$\mathcal{M}(\hat{\mathbf{C}}) = \mathbf{C}(z).$$

Proof. Let $f : \hat{\mathbf{C}} \to \mathbf{C}$ be meromorphic. Then the number of poles of f is finite say at $a_1, \ldots, a_n$. So, locally at a_i we can write

$$f(z) = \sum_{j=1}^{j_i} \frac{\lambda_{j,i}}{(z - a_i)^j} + h_i(z)$$

with h_i holomorphic. Then

$$f(z) - \sum_{i=1}^{n} \sum_{j=1}^{j_i} \frac{\lambda_{j,i}}{(z - a_i)^j}$$

is holomorphic everywhere. By Liouville's theorem this is constant. ■

We say S, S' are isomorphic if $\exists f : S \to S', g : S' \to S$ morphisms such that $f \circ g = \mathrm{id}_{S'}, g \circ f = \mathrm{id}_S$.

Exercise 2.2.9 Show that

$$\hat{\mathbf{C}} \simeq \mathbf{P}^1(\mathbf{C}).$$

Remark 2.2.10 $\mathbf{C} \not\simeq \mathbf{D}$ by Liouville.
If S, S' are connected compact Riemann surfaces, then any nonconstant morphism $f : S \to S'$ is surjective. (Nonconstant holomorphic maps are open)

2.2.4 Ramification

Definition 2.2.11 Orders of vanishing. The **order of vanishing** at $P \in S$ of a holomorphic function on S is defined as follows: For ϕ a chart centered at P write

$$f \circ \phi^{-1}(z) = a_n z^n + a_{n+1} z^{n+1} + \cdots, \; a_n \neq 0$$

then $\mathrm{ord}_P(f) = n$.
More generally, for $f\colon S \longrightarrow S'$ we can define $m_P(f)$ (**multiplicity** of f at P) by using a chart ψ on S' and setting

$$m_P(f) = \mathrm{ord}_P(\psi \circ f).$$

If $m_P(f) \geq 2$ then we call P a **branch point** of f and call f ramified at P. ◊

Example 2.2.12

$$f\colon \mathbf{C} \to \mathbf{C},\; f(z) = z^2.$$

The chart $\phi_a(z) = z - a$ is centered at $a \in \mathbf{C}$. Then to compute $m_a(f)$ we compute

$$f \circ \phi_a^{-1}(z) = a^2 + 2az + z^2$$

hence

$$\mathrm{ord}_a(f) = \begin{cases} 0, & \text{if } a \neq 0 \\ 2, & \text{if } a = 0 \end{cases}.$$

□

2.2.5 Genus

Theorem 2.2.13 Rado. *Any orientable compact surface can be triangulated.*

Fact 2.2.14 *Riemann surfaces are orientable.*

Given such an oriented polygon coming from a Riemann surface, we can associate a word w to it from travelling around the perimeter.

Example 2.2.15 For the sphere $w = a^{-1}ab^{-1}bc^{-1}c$. □

Fact 2.2.16 *Every such word can be normalised without changing the corresponding Riemann surface.*

$$w = \begin{cases} w_0 = aa^{-1}, \\ w_g = a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_g b_g a_g^{-1} b_g^{-1} \end{cases}$$

*The (uniquely determined) g is the **genus** of the surface.*

Example 2.2.17 $w_1 = a_1 b_1 a_1^{-1} b_1^{-1}$.
$w_2 = a_1 b_1 a_1^{-1} b_1 a_2 b_2 a_2^{-1} b_2^{-1}$. □

Theorem 2.2.18

$$\chi(S) = v - e + f = 2 - 2g(S).$$

2.3 Riemann Hurwitz Formula (Sachi)

Exercise 2.3.1 Unimportant. The genus is invariant under changing triangulation.

In particular there are at least two distinct ways of thinking about genus for Riemann surfaces R

1. $$\chi(R) = V - E + F = 2 - 2g$$

2. The dimension of the space of holomorphic differentials on R.

Goal: given R calculate genus

$$y^2 = (x+1)(x-1)(x+2)(x-2)$$

so in an ad hoc way

$$y = \sqrt{(x+1)(x-1)(x+2)(x-2)}$$

when x is not a root of the above we have two distinct values for y, we can imagine two copies of $\mathbf{C}$ sitting above each other and then square root will land in both copies. We have to make branch cuts between the roots and glue along these to account for the fact that going around a small loop surrounding a root will change the sign of our square root. We end up with something looking like a torus here.

Here we examined the value where there were not enough preimages when we plugged in a value for x. The idea is to project to x, and understand the number of preimages.

$$P(x, y) = y^n + p_{n-1}(x)y^{n-1} + \cdots + p_0(x)$$

an irreducible polynomial.

$$R = \{(x, y) : P(x, y) = 0\}.$$

If we fix $x_0 \in \mathbf{P}^1\,\mathbf{C}$ we can analyse how many y values lie over this x. If we have fixed our coefficients we expect n solutions in y over $\mathbf{C}$, i.e. points $(x_0, y) \in R$.

For some values of x_0 this will not be true, there will be fewer y-values, this occurs when we have a multiple root. This happens precisely when the discriminant of this polynomial vanishes, the discriminant is a polynomial and so has finitely many roots.

Definition 2.3.2 Branch points. Let $\pi\colon R \to \mathbf{P}^1\,\mathbf{C}$. We say x_0 is a **branch point** if there are fewer than n distinct y-values above x. Then define the **total branching index**

$$b = \sum_{x\in\mathbf{P}^1\,\mathbf{C}} (\deg(\pi) - \#\pi^{-1}(x)).$$

◊

Claim 2.3.3

$$\chi(R) = \deg \pi \cdot \chi(\mathbf{P}^1\,\mathbf{C}) - b.$$

Lemma 2.3.4 *Locally given some choice of coordinates a non-constant morphism of Riemann surfaces*

$$f\colon R \to S$$

is given by $w \mapsto w^n$. More precisely given $r \in R$, $f(r) = s$ and $V_s \ni s$ a small neighbourhood choose an identification of

$$V_s \xrightarrow{\Psi} D$$

which sends $s \mapsto 0$ and we can find an analytic identification

$$r \in R_r \xrightarrow{\phi} D$$

such that

$$f(U_r) \subseteq V_s.$$

$$\begin{tikzcd} U_r \arrow[r, "f"] \arrow[d, "\phi"'] & V_s \arrow[d, "\Psi"] \\ D \arrow[r, "w \mapsto w^m"'] & D \end{tikzcd}$$

Proof. In Sachi's notes. ■

Proof. Of Claim 2.3.3.

Triangulate R so that every face lies in some small coordinate neighborhood s.t.

$$\pi : R \longrightarrow \mathbf{P}^1\,\mathbf{C}$$

is given by $w \mapsto w^m$, s.t. every edge, all branch points are vertices. This ensures that each face edge and vertex has $n = \deg(\pi)$ preimages (except branch points). Then accounting for branch points we have $\deg(\pi) - \#\pi^{-1}(x_0)$ preimages. ■

Example 2.3.5 $P(x, y)$ plane curve, classically have

$$g = \frac{(d-1)(d-2)}{2}$$

$\mathbf{P}^2 = \{[x : y : z]\}$ and $(\mathbf{P}^2)^* = [a : b : c]$, lines in $\mathbf{P}^2$

$$ax + by + cz = 0$$

and we have lines $\leftrightarrow$ points. We have C^* the dual curve in $\mathbf{P}^2$ cut out by the tangent lines t_Q for $Q \in C$. Claim $\deg C^* = (d-1)d$.
Want

$$R : \{P(x, y) = 0\} \xrightarrow{\pi} \mathbf{P}^1\,\mathbf{C}$$

compute b. In other words, if we fix an arbitrary point $Q \in C$ then there are $d(d-1)$ lines through Q which are tangent to C. Projecting to the x-coordinate $\iff$ family of lines through a point at ∞ $\iff$ $*$ line in $(\mathbf{P}^2)^*$. We have a new question: How many points does this line intersect (up to multiplicity). By bezout $\iff$ $\deg C^*$.
Proof (Matt emerton) Consider a point on C in $\mathbf{P}^2$ such that no tangent line to the curve at ∞ passes through it. Move this point to the origin. If we write

$$P(x, y) = f_d + f_{d-1} + \cdots + f_0$$

then

$$(f_d, f_{d-1}) = 1$$

suppose they share a linear factor:

$$0 = (f_d)_x x + (f_d)_y y + f_{d-1},$$

then this defines a line through the origin. (Because this gives an equation of an asymptote, this is a contradiction).

$$f_d + f_{d-1} + \cdots + f_0 = 0$$

$$d f_d + (d-1) f_{d-1} + \cdots + f_1 = 0$$

$$\Longrightarrow$$

$$\begin{cases} f_d + f_{d-1} + \cdots + f_0 = 0 \\ f_{d-1} + 2 f_{d-2} + \cdots + (d-1) f_1 = 0 \end{cases}.$$

Now these have $d(d-1)$ common solutions. C^* has degree $d(d-1)$ so $b = d(d-1)$. Riemann-Hurwitz implies

$$\chi(R) = 2 \deg \pi - d(d-1)$$

$$\chi(R) = 2d - d(d-1)$$

so

$$g = \frac{(d-1)(d-2)}{2}.$$

□

A 3-fold equivalence of categories. Amazing synthesis.

1. Analysis: Compact connected riemann surfaces.
2. Algebra: Field extensions $K/\mathbf{C}$ where K is finitely generated of transcendence degree 1 over $\mathbf{C}$.
3. Geometry: Complete nonsingular irreducible algebraic curves in $\mathbf{P}^n$.

3) curve $\longrightarrow$ 2) field extension. Over C all rational functions $\frac{P(x)}{Q(x)}$ $\deg P = \deg Q$, $P, Q \colon C \longrightarrow \mathbf{C} \cup \{\infty\}$.
3) $\longrightarrow$ 1) take complex structure induced by $\mathbf{P}^n$.
1) $\longrightarrow$ 2) associated field of meromorphic functions on X.
1) $\longrightarrow$ 3) Any curve which is holomorphic has an embedding into $\mathbf{P}^n$ (Riemann-Roch).
2) $\longrightarrow$ 1) $K/\mathbf{C}$ consider valuation rings R such that $K \supseteq R \supseteq \mathbf{C}$.

Example 2.3.6 $g = 0$, $\mathbf{P}^1$ $\mathbf{C}$ $\mathbf{C}(t)$, $\mathbf{C} \cup \{\infty\}$. □

Example 2.3.7 $g = 1$, elliptic curves, $f(x, y, z)$ smooth plane cubic, $f = 0$, $\mathbf{C}(\sqrt{f(x)}, x)$.

$$\mathbf{C}/\Lambda \longrightarrow \mathbf{P}^2$$

$$z \longmapsto (z, \wp(z), \wp'(z))$$

$$z \notin \Lambda$$

backwards

$$(x, y) \longmapsto \int_{(x_0, y_0)}^{(x,y)} \frac{\mathrm{d}x}{y}$$

□

Riemann-Hurwitz (generally). There's nothing that doesn't generalise about the previous proof.

Claim 2.3.8 *For $\pi\colon R \to S$ a non-constant morphism of compact Riemann surfaces*

$$\chi(R) = \deg \pi \cdot \chi(S) - \sum_{x\in S} (\deg(\pi) - \#\pi^{-1}(x)).$$

Corollary 2.3.9 *There are no non-constant morphisms from a sphere to a surface of genus* > 0.

Proof.

$$f\colon \mathbf{P}^1\,\mathbf{C} \to S$$
$$\chi(\mathbf{P}^1\,\mathbf{C}) = \deg f\,\chi(S) - b$$
$$2 = (+)\cdot(-) - b. \qquad \blacksquare$$

Exercise 2.3.10

$$x^n + y^n + z^n = 0$$

is not solvable in non-constant polynomials for $n > 2$.

Exercise 2.3.11

$$E = \mathbf{C}/\mathbf{Z} + \mathbf{Z}i$$

multiplication by i rotates $x \mapsto xi$ let $x \sim xi$. If we mod out by $\sim$ to get $E/\!\sim$ this is still a Riemann surface and the quotient map

$$f\colon E \to E/\!\sim$$

is nice, compute the branch points of order 4 and order 2.

Exercise 2.3.12 X compact Riemann surface of $g \geq 2$ then there are at most $84(g-1)$ automorphisms of X.

Exercise 2.3.13 Klein quartic

$$x^3y + y^3z + z^3x = 0$$

has 168 automorphisms and is genus 3.

2.4 Riemann Surfaces and Discrete Groups (Rod)

Welcome to BUGLES (Boston university geometry learning expository seminar), the reason it is called bugles is because bugles are hyperbolic, and today we will see a lot of hyperbolic objects.

Plan

1. Uniformization
2. Fuchsian groups
3. Automorphisms of Riemann surfaces

Proposition 2.4.1

$$\mathrm{Aut}(\hat{\mathbf{C}}) = \{z \mapsto \frac{az+b}{cz+d}\}$$
$$\mathrm{Aut}(\mathbf{C}) = \{z \mapsto za + b\}$$
$$\mathrm{Aut}(\mathbf{H}) = \{z \mapsto \frac{az+b}{cz+d}, a, b, c, d \in \mathbf{R}\} = \mathrm{PSL}_2(\mathbf{R})$$

Theorem 2.4.2 *Σ has a universal cover $\widetilde{\Sigma}$ with $\pi_1(\Sigma) = 1$. $\widetilde{\Sigma} \to \Sigma$ holomorphic. $\Sigma = \widetilde{\Sigma}/G$ for $G = \pi_1(\Sigma)$. G acts freely and properly discontinuously.*

2.4.1 Uniformization

Theorem 2.4.3 *The only simply connected Riemann surfaces are $\hat{\mathbf{C}}$, $\mathbf{C}$, $\mathbf{H}$.*

Theorem 2.4.4 *Σ is a Riemann surface then*

$$\begin{aligned} g = 0 &: \Sigma \cong \hat{\mathbf{C}} \\ g = 1 &: \Sigma \cong \mathbf{C}/\Lambda \\ g \geq 2 &: \Sigma \cong \mathbf{H}/K. \end{aligned}$$

Proof. $g = 0$ Uniformization.

$g \geq 1$ $\hat{\mathbf{C}}$ can't be a cover by Riemann-Hurwitz. $g = 1$ $\pi_1(\Sigma) = \mathbf{Z} \oplus \mathbf{Z}$ abelian.

Claim: no subgroup of $\mathrm{Aut}(\mathbf{H})$ is isomorphic to $\mathbf{Z} \oplus \mathbf{Z}$ acting freely and properly discontinuously. So $\widetilde{\Sigma} = \hat{\mathbf{C}}$ $z \mapsto az + b$ free id $a = 1$ so $z \mapsto z + \lambda_1$ $z \mapsto z + \lambda_2$.

$g = 2$ $\pi_1(\Sigma)$ is not abelian but $z \mapsto z + \lambda_1$ is abelian!

$$\Sigma = \mathbf{H}/K,\ K \subsetneq \mathrm{PSL}_2(\mathbf{R}).$$ ∎

Goal. Understand Σ through $\widetilde{\Sigma}$ and G.

Fuchsian groups. $g \geq 2$.

$$\mathrm{Aut}(\mathbf{H}) = \mathrm{PSL}_2(\mathbf{R}) = \mathrm{Isom}^+(\mathbf{H}, \frac{|\,\mathrm{d}z|^2}{\Im Z})$$

hyperbolic $\mathbf{H}$, $\mathbf{D}$ and $\mathrm{PSL}_2(\mathbf{R})$ acts transitively on geodesics.

Definition 2.4.5 Fuchsian groups. A **Fuchsian group** is a discrete subgroup of $\mathrm{PSL}_2(\mathbf{R})$. ◊

Remark 2.4.6 (proof in book) Even if Γ doesn't act freely the quotient

$$\mathbf{H} \to \mathbf{H}/\Gamma$$

is still a covering map and $\mathbf{H}/\Gamma$ is a Riemann surface.

Reflections on H. Say μ is a geodesic in $\mathbf{H}$, i.e. a horocycle. There is $M \in \mathrm{PSL}_2(\mathbf{R})$ with $M\mu$ the imaginary axis. Then $R = -\bar{z}$ is the reflection over the imaginary axis. Now $R_\mu = M^{-1} \circ R \circ M$ is a reflection over μ.

$$R_\mu = \frac{a\bar{z} + b}{c\bar{z} + d} \notin \mathrm{PSL}_2(\mathbf{R})$$

this is a a problem for us.

Triangle groups. Given $n, m, l \in \mathbf{Z} \cup \{\infty\}$ then there is a hyperbolic triangle with angles $\pi/n, \pi/m, \pi/l$ if

$$\frac{1}{n} + \frac{1}{m} + \frac{1}{l} < 1.$$

With area $\pi(1 - \frac{1}{n} - \frac{1}{m} - \frac{1}{l})$.

In the disk model we can start with a wedge of the disk and by adding a choice third geodesic with endpoints on the edge we can adjust the other angles to be what we like.So we can construct hyperbolic triangles with whatever angles we like. Then let R_1 be the reflection over 1 edge, R_2 , R_3 similarly. By reflecting our original triangle T with these reflections we can tessellate the disk, colouring alternately the triangles obtained using an odd or even number of reflections.

The only remaining problem is that R_i's are not in $\mathrm{PSL}_2(\mathbf{R})$. The solution is to define $x_1 = R_3 \circ R_1$, $x_2 = R_1 \circ R_2$, $x_3 = R_2 \circ R_3$ which are all in $\mathrm{PSL}_2(\mathbf{R})$ now. Now we need to take the union of two adjacent triangles before as a fundamental domain, some quadrilateral that still tessellates. So we have formed a Fuchsian group from our triangles.

A presentation for this group is

$$\langle x_1, x_2, x_3 | x_1^n = x_2^m = x_3^l = x_1 x_2 x_3 = 1 \rangle$$

note n, m, l can still be ∞.

Definition 2.4.7 Triangle groups. Let $\Gamma_{n,m,l}$ be the **triangle group** with signature $(1/n, 1/m, 1/l)$. ◊

Remark 2.4.8

$$\frac{1}{n} + \frac{1}{m} + \frac{1}{l} = 1$$

$$\frac{1}{n} + \frac{1}{m} + \frac{1}{l} > 1$$

still work on $\mathbf{C}$ and $\hat{\mathbf{C}}$ respectively.

Example 2.4.9 $\mathrm{PSL}_2(\mathbf{Z})$**.** Consider $\Gamma_{2,3,\infty}$ angles $\pi/2, \pi/3, 0$. We can draw such a triangle in the upper half plane with vertices $i, e^{\pi i/3}, \infty$. So a fundamental domain will be the region obtained by reflecting through the imaginary axis, given by $-\frac{1}{2} \leq \Re z \leq \frac{1}{2}$, $|z| \geq 1$. We have $R_1 = \frac{1}{\bar{z}}, R_2 = -\bar{z} + 1, R_3 = -\bar{z}$ so $x_1 = \frac{-1}{z}, x_2 = \frac{1}{-z+1}, x_3 = z + 1$. Then $\Gamma_{2,3,\infty} \cong \mathrm{PSL}_2(\mathbf{Z})$. Sometimes denoted $\Gamma(1)$. □

Observation 2.4.10 If $\Gamma_1 < \Gamma_2$ and T is a fundamental domain of Γ_2 then if $\gamma_1, \gamma_2, \ldots, \gamma_n \in \Gamma_2$ are representatives of $\Gamma_1 \backslash \Gamma_2$ then

$$\bigcup \gamma_i(T)$$

is a fundamental domain for Γ_1.

Example 2.4.11 $\Gamma(1)$**.**

$$\Gamma(2) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{id} \pmod 2\}$$

then

$$[\Gamma(1) : \Gamma(2)] = 6$$

representatives of $\Gamma(2)\backslash\Gamma(1)$ are

$$x_1 = \mathrm{id},\ x_2 = \frac{-1}{z-1}, x_3 = \frac{z-1}{z},\ x_4 = \frac{z-1}{z},\ x_5 = \frac{-z}{x-1},\ x_6 = \frac{-1}{z}.$$

Lets see what these do, for example if $z = e^{i\theta}$

$$\Re(x_2(z) = \frac{-1}{e^{i\theta}-1} = \frac{-e^{i\theta}+1}{2-2\cos\theta}) = \frac{1-\cos\theta}{2-2\cos\theta}\frac{1}{2}$$

if we plot this we see we get two copies of a 0,0,0 triangle so this corresponds to $\Gamma_{\infty,\infty,\infty}$.

$$\langle x_1, x_2, x_3 | x_1x_2x_3 = 1\rangle = \langle x_1, x_2\rangle = \pi_1(\mathbf{P}^1 \setminus \{0,1,\infty\}).$$

$\square$

Proposition 2.4.12 $S_1 = \mathbf{H}/\Gamma_1$, $S_2 = \mathbf{H}/\Gamma_2$ *then*

$$S_1 \cong S_2 \iff \Gamma_1 = T \circ \Gamma_2 \circ T^{-1},\ T \in \mathrm{PSL}_2(\mathbf{R}).$$

Proof. $\Leftarrow$ Define an $\phi\colon S_1 \to S_2$ via $\phi([z]_1) = [T(z)]_2$.
$\Rightarrow$ Take a lift

$$\begin{tikzcd} \mathbf{H} \arrow[r, "\tilde{\phi}"] \arrow[d] & \mathbf{H} \arrow[d] \\ \mathbf{H}/\Gamma_1 \arrow[r, "\phi"'] & \mathbf{H}/\Gamma_2 \end{tikzcd}$$

then $T = \tilde{\phi}$. $\blacksquare$

Proposition 2.4.13 Γ *a* *Fuchsian group* *acts freely*

$$\mathrm{Aut}(\mathbf{H}/\Gamma) = N(\Gamma)/\Gamma.$$

Proof. Previous proposition, set $\Gamma_1 = \Gamma_2$

$$N(\Gamma) \to \mathrm{Aut}(\mathbf{H}/\Gamma)$$

kernel is Γ. $\blacksquare$

Corollary 2.4.14 *Let* Σ *be a* *Riemann surface* *with* $g \geq 2$ *then*

$$|\,\mathrm{Aut}(\Sigma)| < \infty.$$

Proof.

$$\begin{tikzcd} \mathbf{H} \arrow[d, "\phi_2"'] \arrow[dr, "\phi_1"] & \\ S = \mathbf{H}/\Gamma \arrow[r, "f"'] & \mathbf{H}/N(\Gamma) = S/\mathrm{Aut}(S) \end{tikzcd}$$

since ϕ_1, ϕ_2 are holomorphic then so is f. So $\deg f = |N(\Gamma)/\Gamma|$ and $\deg f < \infty$. $\blacksquare$

Say Σ, $g \geq 2$, $G \subseteq \mathrm{Aut}(\Sigma)$. Let $\bar{g}$ be the genus of Σ/G

$$2g-2 = |G|(2\bar{g}-2) + \sum_p (I(p)-1) = |G|(2\bar{g}-2+\sum_{i=1}^{n}(1-\frac{1}{|I(p_i)|}))$$

where $I(p)$ is the stabiliser of p in G and $\{p_i\}$ area maximal set of fixed points of G inequivalent under the action of G.

Exercise 2.4.15 Σ, $g \geq 2$ then $|\operatorname{Aut}(\Sigma)| \leq 84(g-1)$. Hint: cases.

Exercise 2.4.16 Consider

$$1 \longrightarrow \Gamma(n) \longrightarrow \Gamma(1) \longrightarrow \mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z}) \longrightarrow 1$$

compute genus of $\mathbf{H}/\Gamma(n)$.

2.5 Riemann Surfaces and Discrete Groups II (Jim)

2.5.1 Moduli space of compact Riemann surfaces with genus g

$g = 0$. Uniformization tells us that up to isomorphisms all Riemann surfaces of genus 0 are $\mathbf{P}^1$ hence the moduli space $\mathcal{M}_0 = \{\mathrm{pt}\}$.

$g = 1$. Uniformization tells us that each Riemann surface of genus 1 is a torus and can be written as $\mathbf{C}/\omega_1\mathbf{Z} + \omega_2\mathbf{Z} \longrightarrow \mathbf{C}/(\mathbf{Z} \oplus \tau\mathbf{Z})$, with $\tau = \pm\omega_1/\omega_2$.

Proposition 2.5.1 2.54.

$$\mathcal{M}_1 \simeq \mathbf{H}/\mathrm{PSL}_2(\mathbf{Z}) \simeq \mathbf{C}.$$

Proof. Idea: Existence of

$$\mathbf{C}/\Lambda_{\tau_1} \xrightarrow{\sim} \mathbf{C}/\Lambda_{\tau_2}$$

with $\bar{T}([0]) = [0]$ is equivalent to the existence of $T \in \operatorname{Aut}(\mathbf{C})$ (choose $T(z) = wz$) such that $w(\mathbf{Z} \oplus \tau_1\mathbf{Z}) = \mathbf{Z} \oplus \tau_2\mathbf{Z}$. This in turn is equivalent to the existence of

$$A, A' \in \mathrm{GL}_2(\mathbf{Z})$$

s.t. $\det(A) = \det(A') = \pm 1$ so that

$$\begin{pmatrix} w \\ w\tau_1 \end{pmatrix} A \begin{pmatrix} 1 \\ \tau_2 \end{pmatrix} = A' \begin{pmatrix} w \\ w\tau_1 \end{pmatrix}$$

$$\implies \tau_q = A\psi_2 = \frac{a\tau_2 + b}{c\tau_2 + d}$$

and $A \in \mathrm{PSL}_2(\mathbf{R})$. Implies $A \in \mathrm{PSL}_2(\mathbf{Z})$ as both $\tau_1, \tau_2 \in \mathbf{H}$. Conversely if

$$\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + b}$$

isomorphism is induced by $T(z) = (c\tau_2 + d)z$. ∎

$g > 1$ $\mathcal{M}_g$ is a complex variety of dimension $3g-3$. Uniformization tells us that describing a Riemann surface amounts to specifying $2g$ real 2×2 matrices $\{\gamma_i\}_{i=1}^{2g}$ such that

1. $\det(\gamma_i) = 1$ which implies that γ_i depends on 3 real parameters so we have a total of $6g$.

2. $\prod_{i=1}^{g}[\gamma_i, \gamma_{g+i}] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 3 relations, so $6g-3$. Since for any $\gamma \in \mathrm{PSL}_2(\mathbf{R})$ $\Gamma = \langle\gamma_i\rangle$ and $\gamma\Gamma\gamma^{-1}$ uniformize isomorphic Riemann surfaces implies $6g-6$ real parameters, so $3g-3$ complex parameters.

2.5.2 Monodromy

Let $f\colon S_1 \longrightarrow S$ be a morphism of degree d ramified over $y_1, \dots, y_n \in S$. For $y \in S \setminus \{y_1, \dots, y_n\}$ we have a group homomorphism

$$M_f\colon \pi_1(S \setminus \{y_1, \dots, y_n\}) \longrightarrow \mathrm{Bij}(f^{-1}(y))$$
$$\gamma \longmapsto M_f(\gamma) = \sigma_\gamma^{-1}.$$

σ_γ is defined as follows:

$$\gamma \in \pi_1(S \setminus \{y_1, \dots, y_n\})$$

lifts to a path $\widetilde{\gamma}$ from $x \in f^{-1}(y)$ to another $x' \in f^{-1}(y)$ set $\sigma_\gamma(x) = x'$. If we number the points in $f^{-1}(y)$ we may think of $M_f(\pi_1) \subseteq \Sigma_d$, via some $\phi\colon \{1, \dots, d\} \longrightarrow f^{-1}(y)$. $\mathrm{Mon}(f)$ is the image of $M_f(\pi_1)$ in Σ_d.

Monodromy and Fuchsian groups. Let

$$\pi\colon \mathbf{H}/\Gamma_1 \longrightarrow \mathbf{H}/\Gamma$$

be the Fuchsian group representation of the map

$$f\colon S_1 \longrightarrow S \ni y.$$

Identifications $y = [z_0]_\Gamma$ for some $z_0 \in \mathbf{H}$.

$$\pi_1(S \setminus \{y_1, \dots, y_n\}) \simeq \Gamma$$
$$f^{-1}(y) = \{[\beta z_0]_{\Gamma_1}\}$$

where β runs along a set of representatives of $\Gamma_1 \backslash \Gamma$.

$$M_f\colon \Gamma \longrightarrow \mathrm{Bij}(\Gamma_1 \backslash \Gamma)$$
$$\gamma \longmapsto M_f(\gamma)$$
$$\Longrightarrow \gamma \sim \pi_1([z_0, \gamma(z_0)])$$

where $[z_0, \gamma(z_0)]$ is a path in $\mathbf{H}$. Lift this loop to $\mathbf{H}/\Gamma_1$ is the path $\pi_{\Gamma_1}(\beta[z_0, \gamma_0(z_0)])$. which corresponds to $\Gamma_1\beta\gamma$, this implies $\sigma_\gamma(\Gamma_1\beta) = \Gamma_1\beta\gamma$.

Corollary 2.5.2 2.59.

$$M_\pi\colon \Gamma \longrightarrow \mathrm{Bij}(\Gamma_1 \backslash \Gamma)$$

induces an isomorphism

$$\frac{\Gamma}{\bigcap_{\beta \in \Gamma_1} \beta^{-1}\Gamma_1\beta} \simeq \mathrm{Mon}(\pi)$$

characterize morphisms by monodromy. Let f_i have degree 2, non conjugate.

Proposition 2.5.3 2.63. *For S a compact Riemann surface and $\beta = \{a_1, \dots, a_n\} \subset S$ for some $d \geq 1$ there are only finitely many pairs $(\tilde{S}, f)$ where $\tilde{S}$ is a compact Riemann surface and*

$$f\colon \tilde{S} \longrightarrow S$$

is a degree d morphism with branching value set β.

Proof. Special case: Assume $S = \mathbf{P}^1$ and $n = 3$.

$$\Gamma = \Gamma(2) = \{A \in \mathrm{PSL}_2(\mathbf{Z}) : A = \mathrm{id} \pmod 2\}$$
$$= \pi_1(S' \setminus \{0, 1, \infty\})$$

is generated by γ_1, γ_2 so any map $M_f\colon \Gamma(2) \longrightarrow \Sigma_d$ is determined by images of γ_1, γ_2. ∎

2.5.3 Galois coverings

Definition 2.5.4 A covering $f\colon S_1, \to S_2$ is Galois (or regular, or normal) if the covering group

$$\mathrm{Aut}(S, f) = \{h \in \mathrm{Aut}(S_1) : f \circ h = f\} = G$$

acts transitively on each fibre. With this notion we can think of $S_1 \to S_1/G$. ◊

Proposition 2.5.5 2.65.

$$f\colon S_1 \to S_2$$

is Galois if and only if

$$f^*\colon M(S_2) \to M(S_1)$$

is a Galois extension. In this case $\mathrm{Aut}(S_1, f) \simeq \mathrm{Gal}(M(S_1)/M(S_2))$.

Example 2.5.6 Hyperelliptic covers of $\mathbf{P}^1$ given by

$$S = \{y^2 = \prod_{i=1}^{N}(x - a_i)\} \to \mathbf{P}^1$$

$$(x, y) \to x$$

covering group G is order 2 generated by the involution $J(x, y) = (x, -y)$. □

Proposition 2.5.7 2.66. *A covering*

$$f\colon S_1 \to S_2$$

is normal/Galois iff

$$\deg(f) = |\mathrm{Mon}(f)|.$$

2.5.4 Normalization of coverings of $\mathbf{P}^1$

Let $f\colon S \to \mathbf{P}^1$ be a cover of deg $d > 0$ with $\mathrm{Mon}(f) \leq \Sigma_d$.

The normalisation

$$\tilde{f}\colon \tilde{S} \to \mathbf{P}^1$$

associated to f has $\mathrm{Mon}(f) \cong \mathrm{Aut}(\tilde{S}, \tilde{g}$ and $\tilde{f}^*\colon M(\mathbf{P}^1) \to M(\mathbf{P}^1)$ is the normalisation of the extension

$$f^*\colon M(\mathbf{P}^1) \hookrightarrow M(S)$$

Normalization of extensions $K \hookrightarrow L$ is a Galois extension of K of lowest possible degree containing L.

Definition 2.5.8 Normalization of $f\colon S \to \mathbf{P}^1$ deg $d > 0$ is a Galois covering $\tilde{f}\colon \tilde{S} \to \mathbf{P}^1$ of lowest possible degree s.t. $\exists \pi\colon \tilde{S} \to S$ with the diagram commuting. ◊

Corollary 2.5.9 2.73.

$$\mathrm{Mon}(f) \simeq \mathrm{Aut}(\tilde{S}, \tilde{f})$$

Interpretation in terms of Fuchsian groups:

Proposition 2.5.10 *Let* $f\colon S_1 \to S$ *be a covering of Riemann surfaces* $S_1 \setminus f^{-1}\{y_1, \ldots, y_n\} \to S \setminus \{y_1, \ldots, y_n\}$. *The unramified cover and* $\pi\colon \mathbf{H}/\Gamma_1 \to \mathbf{H}/\Gamma$ *the Fuchsian group representatives. The normalisation of* f *can be represented as the* *compactification of*

$$\mathbf{H}/\bigcap_{\gamma\in\Gamma}\gamma^{-1}\Gamma_1\gamma \longrightarrow \mathbf{H}/\Gamma_1 \longrightarrow \mathbf{H}/\Gamma$$

so the covering group is isomorphic to $\Gamma/\bigcap\gamma^{-1}\Gamma_1\gamma \simeq \mathrm{Mon}(f)$.

Example 2.5.11 Let $F(x,y) = y^2x - (y-1)^3$ consider

$$S_F \longrightarrow \mathbf{P}^1$$

$$(x,y) \longrightarrow x$$

S_F has genus 0. $S_F \longrightarrow \mathbf{P}^1$ is of degree 3 and ramified at most over $0, \frac{-27}{4}, \infty$. $\mathrm{Mon}(x) \simeq \Sigma_3$ so not a normal covering. Normalization of (S_F, x) is $S_{\tilde{F}}, \tilde{x})$ where

$$\tilde{F}(x,y) = y^2(1-y)^2x + (1-y+y^2)$$

□

2.6 Belyi's theorem (Maria)

Theorem 2.6.1 *Let S be a compact riemann surface, then the following are equivalent.*

1. *S is defined over $\overline{\mathbf{Q}}$ (iff over a number field)*
2. *S admits a morphism $f\colon S \longrightarrow \mathbf{P}^1$ with at most 3 branching values.*

Definition 2.6.2 Belyi functions. A meromorphic function with less than 4 branching values is a **Belyi function**. ◊

Remark 2.6.3

1. Branching values can be taken to be in $\{0,1,\infty\}$.
2. If $S \neq \mathbf{P}^1$, then $f\colon S \longrightarrow \mathbf{P}^1$ has at least 3 branching values

Definition 2.6.4 Belyi polynomials. Let $m,n \in \mathbf{N}$, $\lambda = m/(m+n)$, define

$$P_\lambda(x) = P_{m,n}(x) = \frac{(m+1)^{m+n}}{m^m n^n}x^m(1-x)^n$$

Belyi polynomials. ◊

Proposition 2.6.5 *P_λ satisfies*

1. *P_λ ramifies at exactly $0,1,\lambda,\infty$.*
2. *$P_\lambda(0) = P_\lambda(1) = 0, P_\lambda(\lambda) = 1, P_\lambda(\infty) = \infty$.*

Example 2.6.6

$$S_\lambda : y^2 = x(x-1)(x-\lambda)$$

with $\lambda = m/(m+n)$. From ex. 1.32

$$x\colon S_\lambda \longrightarrow \mathbf{P}^1$$

$$(x,y) \mapsto x$$

$$\infty \mapsto \infty$$

ramifies over $0, 1, \lambda, \infty$. Then $f = P_\lambda \circ x \colon S_\lambda \to \mathbf{P}^1$ ramifies exactly at $(0, 0), (1, 0), (\lambda, 0), \infty$. With branching values $0, 0, 1, \infty$ so that f is a Belyi function. $\square$

2.6.1 Proof of a) implies b)

Note 2.6.7 Its enough to show $\exists f \colon S \to \mathbf{P}^1$ ramified over $\{0, 1, \infty, \lambda_1, \dots, \lambda_n\} \subseteq \mathbf{Q} \cup \{\infty\}$. Given this we can repeatedly use Belyi polynomials to obtain $g \colon S \to \mathbf{P}^1$ ramified over $\{0, 1, \infty\}$.

Write $S = S_F$

$$F(x, y) = p_0(x)y^n + \cdots + p_n(x)$$

defined over $\overline{\mathbf{Q}}[x, y]$. Let $B_0 = \{\mu_1, \dots, \mu_s\}$ be the branching values of $x \colon S_F \to \mathbf{P}^1$.

Theorem 1.86 says that the each μ_i is ∞, a root of $p_0(x)$ or a common root of F, F_y which implies by lemma 1.84 that $B_0 \subseteq \overline{\mathbf{Q}} \cup \{\infty\}$. If $B_0 \subseteq \mathbf{Q} \cup \{\infty\}$ we are done otherwise let $m_1(T) \in \mathbf{Q}[T]$ be the minimal polynomial of $\{\mu_1, \dots, \mu_s\}$. Let $\{\beta_1, \dots, \beta_d\}$ be the roots of $m_1'(T)$ and $p'(T)$ their min. poly. Note : $\deg P(t) < \deg m_1'(T)$

Note: $\mathrm{Branch}(g \circ f) = \mathrm{Branch}(g) \cup g(\mathrm{Branch}(f))$ branching values.

So B_1 $\mathrm{Branch}(m_1 \circ x) = m_1(\{\text{roots of } m_1'\}) \cup \{0, \infty\}$.

$$S \xrightarrow{x} \mathbf{P}^1 \xrightarrow{m_1} \mathbf{P}^1$$

If $B_1 \subseteq \mathbf{Q} \cup \{\infty\}$ done. Otherwise let $m_2(T)$ be the minimal polynomial $/\mathbf{Q}$ of $\{m_1(\beta_1), \dots, m_1(\beta_d)\}$, $B_2 = \mathrm{Branch}(m_2 \circ m_2 \circ x)$. Fact: $\deg(m(t)) < \deg(m_1(T))$.

Repeat inductively until $B_k \subseteq \mathbf{Q} \cup \{\infty\}$ which is guaranteed by the decreasing degrees.

2.6.2 Algebraic characterization of morphisms

Proposition 2.6.8 *Defining a morphism $f \colon S_F \to S_G$ is equivalent to giving a pair of rational functions*

$$f = (R_1, R_2),\ R_i = \frac{P_i}{Q_i},\ P_i, Q_i \in \mathbf{C}[x, y],\ Q_i \notin (F)$$

such that $Q_1^{\deg_x(G)} Q_2^{\deg_y(G)} G(R_1, R_2) = HF$ for some $H \in \mathbf{C}[x, y]$. $f(R_1, R_2)$ is an isomorphism if there exists an inverse morphism $h \colon S_G \to S_F$.

Remark 2.6.9

$$\begin{tikzcd} S_f \arrow[r, "f"] \arrow[dr, "m"'] & S_G \arrow[d, "h"] \\ & S_D \end{tikzcd}$$

The fact that this diagram commutes can be expressed by polynomial identities.

2.6.3 Galois action

Let $\mathrm{Gal}(\mathbf{C}) = \mathrm{Gal}(\mathbf{C}/\mathbf{Q})$.

Definition 2.6.10 For $\sigma \in \mathrm{Gal}(\mathbf{C})$, $a \in \mathbf{C}$ denote $a^\sigma = \sigma(a)$,

1. If $P = \sum a_{ij}x^i y^j \in \mathbf{C}[x,y]$ set
$$P^\sigma = \sum a_{ij}^\sigma x^i y^j \in \mathbf{C}[x,y]$$
if $R = P/Q$ set $R^\sigma = P^\sigma/Q^\sigma$.
2. If $S \simeq S_F$, $S^\sigma = S_{F^\sigma}$.
3. If $\Psi = (R_1, R_2)\ S_F \longrightarrow S_G$ is a morphism, set $\Psi^\sigma = (R_1^\sigma, R_2^\sigma)\colon S_{F^\sigma} \longrightarrow S_{G^\sigma}$.
4. For an equivalence class $(S, f) = (S_F, R(x,y))$ of ramified covers of $\mathbf{P}^1$ set $(S,f)^\sigma = (S^\sigma, f^\sigma) = (S_{F^\sigma}, R^\sigma(x,y))$.

◊

Exercise 2.6.11 Verify this Galois action is well-defined (lemma 3.12).

Recall: S_F is constructed from a noncompact Riemann surface $S_F^\times \subseteq \mathbf{C}^2$ by adding finitely many points, (theorem 1.86). If $P = (a,b) \in S_F^\times$ then $P^\sigma = (a^\sigma, b^\sigma)$. What about the other points?

2.6.4 Points and valuations

Definition 2.6.12 Let $\mathcal{M}$ be a function field. A (discrete) valuation of $\mathcal{M}$ is $v\colon \mathcal{M}^* \to \mathbf{Z}$ s.t.

1. $v(\phi\psi) = v(\phi) + v(\psi)$
2. $v(\phi \pm \psi) \geq \min\{v(\phi), v(\psi)\}$
3. $v(\phi) = 0$ if $\phi \in \mathbf{C}^*$
4. v is nontrivial $\exists \phi : v(\phi) \neq 0$

set $v(0) = \infty$. ◊

Facts:
$$A_v = \{\phi \in \mathcal{M} : v(\phi) \geq 0\} \subseteq \mathcal{M}$$
is a subring that is a local ring with a maximal ideal
$$M_v = \{\phi \in \mathcal{M} : v(\phi) > 0\} = (\phi)$$
for some ϕ a uniformizer.

If $v(\phi) = 1$ v is normalised.

Proposition 2.6.13 3.15. *Every point $P \in S$ a compact Riemann surface defines a valuation on $\mathcal{M}(S)$ by $v_P(\phi) = \mathrm{ord}_P(\phi)$.*

Proof. Easy exercise. ■

Theorem 2.6.14 3.23. *For any compact Riemann surface S*
$$P \in S \mapsto v_P = \mathrm{ord}_P$$
gives a 1-1 correspondence between points of S and normalised valuations on $\mathcal{M}(S)$.

Proof. Sketch: First prove it for $S = \mathbf{P}^1$.

Inductively meromorphic functions separate points.

Surjectivity study behaviour of valuations in finite extensions of fields and use a nonconstant morphism $f : S \to \mathbf{P}^1$ to reduce to the case of $\mathbf{P}^1$. ∎

Galois action on points.
Definition 2.6.15

1. Given a valuation v on $\mathcal{M}(S)$ define a valuation v^σ on $\mathcal{M}(S^\sigma)$ by $v^\sigma = v \circ \sigma^{-1}$ i.e. $v^\sigma(\psi^\sigma) = v(\psi)$ for all $\psi \in \mathcal{M}(S)$.
2. For $P \in S$ define $P^\sigma \in S^\sigma$ as the unique point in S^σ s.t. $v_{P^\sigma} = (v_P)^\sigma$.

◊

Proposition 2.6.16 3.25.

1. *For $\sigma \in \mathrm{Gal}(\mathbf{C})$, $P \mapsto P^\sigma$ is a bijection $S \to S^\sigma$.*
2. *On $P \in S_F^\times$ this agrees with the previous definition of P^σ.*
3. *$a^\sigma = a$ for all $a \in \mathbf{Q} \cup \{\infty\}$ for all $\sigma \in \mathrm{Gal}(\mathbf{C})$.*

Proof. Sketch

1. $a \mapsto a^{\sigma^{-1}}$.
2. Follows as in proof of 3.22
3. Obvious for $a \in \mathbf{Q}$, for ∞:
$$(v_\infty)^\sigma(x-1) = v_\infty(x - a^{\sigma^{-1}}) = 1 = v_\infty(x-1)$$
for all $a \in \mathbf{C}$ implies $(v_\infty)^{\sigma^{-1}} = v_\infty$ implies $\infty^\sigma = \infty$.

∎

2.6.5 Elementary invariants of the action of $\mathrm{Gal}(\mathbf{C})$.

Remark 2.6.17 The bijection $S \leftrightarrow S^\sigma$ is not holomorphic. In general S and S^σ are not isomorphic.

Theorem 2.6.18 *The action of* $\mathrm{Gal}(\mathbf{C})$ *on pairs* (S, f) *satisfies*

1. $$\deg(f^\sigma) = \deg(f)$$
2. $$(f(P))^\sigma = f^\sigma(P^\sigma)$$
3. $$\mathrm{ord}_{P^\sigma}(f^\sigma) = \mathrm{ord}_P(f)$$
4. *$a \in \hat{\mathbf{C}}$ is a branching value of f iff a^σ is a branching value of f^σ.*
5. $\mathrm{genus}(S) = \mathrm{genus}(S^\sigma)$ *i.e. they are homeomorphic.*
6. $\mathrm{Aut}(S, f) \to \mathrm{Aut}(S^\sigma, f^\sigma)$ *via $h \mapsto h^\sigma$ is a group homomorphism.*
7. *The monodromy group* $\mathrm{Mon}(f)$ *of* (S, f) *is isomorphic to* $\mathrm{Mon}(f^\sigma)$ *of* (S^σ, f^σ).

We will use properties 1 and 4 at least.

Proposition 2.6.19 Criterion 3.29. *For a compact Riemann surface S the following are equivalent*

1. *S is defined over $\overline{\mathbf{Q}}$.*
2. *$\{S^\sigma\}_{\sigma\in \mathrm{Gal}(\mathbf{C})}$ contains only finitely many isomorphism classes of Riemann surfaces.*

Proof. 1 implies 2: $S = S_F$, $F = K[x, y]$ for K a number field then

$$|\{F^\sigma\}_{\sigma\in \mathrm{Gal}(\mathbf{C})}| \leq [K : \mathbf{Q}]$$

2 implies 1 is section 3.7. ∎

Proof of b implies a in Belyi's theorem (3.61). Suppose $f : S \longrightarrow \mathbf{P}^1$ is a morphism of degree d with branching values $\{0, 1, \infty\}$. By theorem 3.28 $\forall\sigma \in \mathrm{Gal}(\mathbf{C})$

$$f^\sigma : S^\sigma \to \mathbf{P}^1$$

is a morphism of degree d and branching values are

$$\{\sigma(0), \sigma(1), \sigma(\infty)\} = \{0, 1, \infty\}.$$

So $\{f^\sigma\}_{\sigma\in \mathrm{Gal}(\mathbf{C})}$ gives rise to only finitely many monodromy homomorphisms.

$$F_{f^\sigma} : \pi_1(\mathbf{P}^1 \setminus \{0, 1, \infty\}) \longrightarrow \Sigma_d$$

the fundamental group is free on two generators so there are only finitely many such maps. Theorem 2.61 implies $\{S^\sigma\}_{\sigma\in \mathrm{Gal}(\mathbf{C})}$ contains only finitely many equivalence classes so by the criterion S is defined over $\overline{\mathbf{Q}}$.

2.6.6 The field of definition of Belyi functions (3.8)

Proposition 2.6.20 *Belyi functions are defined over $\overline{\mathbf{Q}}$.*

Proof. Use the same methods as in 3.7. ∎

2.7 Dessins (Berke)

$$G_{\mathbf{Q}} \circlearrowleft (X, D) \leftrightarrow (S, f) \circlearrowright G_{\mathbf{Q}}$$

where (X, D) is a dessin, (S, f) is a Belyi pair.

2.7.1 Dessins

Definition 2.7.1 A dessin is a pair (X, D) where X is an oriented compact topological surface and $D \subset X$ is a finite graph:

1. D is connected
2. D is bicoloured
3. $X \setminus D$ is a disjoint union of topological disks.

◊

Not all of these are so important (for example 3 implies 1 (but the converse does not hold)). We can also obtain a bicoloured graph from an uncoloured graph by subdividing all edges and colouring the new vertices black and the others white.

A single edge in a sphere is, a single edge in a torus is not.

Permutation representation of a Dessin. Label the edges of a dessin $\{1, \dots, N\}$ then

$$\sigma_0(i) = \text{subsequent edge in the cycle around the white vertex of } i$$

as we have a positive orientation on the edges

$$\sigma_1(i) = \text{subsequent edge in the cycle around the black vertex of } i.$$

Then we define

Definition 2.7.2 (σ_0, σ_1) is the permutation representation pair of (X, D). ◊

Say

$$\sigma_0 = (1, \dots, N_1)(N_1 + 1, \dots, N_2) \cdots$$

a product of disjoint cycles. Then each of these cycles corresponds to a white vertex, where the length of the cycle is the degree of the corresponding vertex. Same for σ_1 and black vertices.

$$\{\text{cycles appearing in the decomposition of } \sigma_0\sigma_1\}$$
$$\updownarrow$$
$$\{\text{faces of } D\}$$

Exercise 2.7.3 Prove this.

Remark 2.7.4 D connected implies that $\langle \sigma_0, \sigma_1 \rangle$ is transitive on Σ_N. As D is bicoloured the cycles on D contain an even number of edges.

A dessin is not a triangulation of X but

$$\chi(X) = \#V - \#E + \#F$$

proof later.

Proposition 2.7.5

$$\chi(X) = (\#\textit{cycles of } \sigma_0 + \#\textit{cycles of } \sigma_1) - N + \#\{\textit{cycles of } \sigma_0\sigma_1\}.$$

$$(\sigma_0, \sigma_1) \rightsquigarrow (X', D)$$
$$\langle \sigma_0, \sigma_1 \rangle \subseteq \Sigma_N$$

is transitive.

Proposition 2.7.6 *There exists* (X, D) *with permutation representation* (σ_0, σ_1).

Proof. Write $\sigma_0\sigma_1 = \tau_1 \cdots \tau_k$, τ_i disjoint cycles each of length n_i with $\sum n_i = N$. Create k faces bounded by $2n_1, \dots, 2n_k$ vertices, and assign the vertices white and black colours so that the graph is bicoloured. As $\sigma_0\sigma_1$ should jump two each time we get an identification of all edges which we then glue using σ_0. ∎

Definition 2.7.7 We say that

$$(X_1, D_1) \sim (X_2, D_2)$$

if there exists an orientation preserving homeomorphism $\phi\colon X_1 \to X_2$, $\phi|_{D_1}\colon D_1 \xrightarrow{\sim} D_2$. ◊

Theorem 2.7.8

$$\{\textit{Dessins}\}/\!\sim\leftrightarrow \{(\sigma_0, \sigma_1),\ \langle\sigma_0, \sigma_1\rangle \subseteq \Sigma_N \textit{ transitive}\}/\!\sim$$

2.7.2 Dessins 2 Belyi pairs

Triangle decomposition of $(X, D) \rightsquigarrow T(D)$ a set of triangles that cover D and intersect along edges or at vertices.

Example 2.7.9 Edge in the sphere, add an extra vertex $\times$ not on the edge and get a decomposition into two triangles. □

We will label triangles by $T_j^{\pm}$ as there are two for each edge, by orientation some are the same.

$$T(D) \rightsquigarrow f_D\colon X \to \hat{\mathbf{C}}$$

Glue

$$f_j^?\colon T_j^? \to \overline{\mathbf{H}}^?$$

for $? \in \{+, -\}$, where $f_j^+ = f_j^-$ on the intersection. Where $\partial T_j \xrightarrow{\sim} \mathbf{R} \cup \{\infty\}$

$$\text{black} \mapsto 0$$

$$\text{white} \mapsto 1$$

$$\times \mapsto \infty$$

and we have $\mathrm{Branch}(f_D) \subseteq \{0, 1, \infty\}$. Now $\deg f_D = \#\text{edges of } D$, $m_v(f_D) = \deg v$, $f_D^{-1}([0, 1]) = D$. Modify X a little bit and use some lemma to get $S_D \simeq_{\text{top}} X$ for some Riemann surface with $f_D\colon S_D \to \mathbf{P}^1$.

Definition 2.7.10 (S, f) is a Belyi pair with S compact Riemann surface and f a Belyi function on S.

$$(S_1, f_1) \sim (S_2, f_2)$$

if it is an isomorphism of ramified coverings. ◊

So we can now go in both directions.

$$\{\text{Dessins}\}/\!\sim$$

$$\updownarrow$$

$$\{\text{Belyi pairs}\}/\!\sim$$

$$(X, D) \mapsto (S_D, f_D)$$

$$(S, D_f) \leftarrow\!\shortmid (S, f)$$

Now to define the Galois action

$$G_{\mathbf{Q}} \circlearrowright \{\text{Dessins}\} \leftrightarrow \{\text{Belyi pairs}\}$$

$$\begin{tikzcd}
(X, D) \arrow[r, dashed] \arrow[d] & (X, D)^\sigma \\
(S_D, f_D) \arrow[r] & (S_D^\sigma, f_D^\sigma)^\sigma \arrow[u]
\end{tikzcd}$$

The $G_{\mathbf{Q}}$ action is faithful on dessins of genus g.

Example 2.7.11 Same example $\mathbf{P}^1$ with a single edge, $f_D = z$, $\deg f_D = \#$ edges, $m_v(f) = \deg v$. □

Exercise 2.7.12 String.

Exercise 2.7.13 n star.

2.8 A Sandwich Table of Dessins d'Enfants

Alex: So I haven't typed this section as it was a lot of pictures and I haven't got nice scans of them, will try at some point (maybe?). Angus' notes can be found at `http://math.bu.edu/people/angusmca/buntes/spring2018.html`.

2.9 Belyi's theorem, effective Mordell and ABC (Angus)

We begin with one of the most famous results in arithmetic geometry.

Theorem 2.9.1 Mordell conjecture/Falting's theorem. *Let C be an algebraic curve of genus ≥ 2 over a number field K. Then $C(K)$ is finite.*

There are many proofs of this, Falting's being the original and most famous.

Remark 2.9.2 Falting's proof is not effective. That is, it cannot predict the number of points or give any bounds.

Today we'll show how this theorem follows from a (much harder conjecture), but how this nonetheless gives new insight into the question of effectiveness. Specifically we'll show ABC implies Mordell.

"Mordell is as easy as ABC"- Zagier

Conjecture 2.9.3 ABC. *Let $A, B, C \in \mathbf{Z}$ s.t. $\gcd(A, B, C) = 1$ and $A + B + C = 0$, then for all $\epsilon > 0$ there exists a constant k_ϵ s.t.*

$$N(A, B, C) > k_\epsilon H(A, B, C)^{1-\epsilon}$$

where

$$N(A, B, C) = \prod_{p \mid ABC} p$$

$$H(A, B, C) = \max(|A|, |B|, |C|).$$

This is a remarkably deep statement about the integers. Something surprising about how one compares the additive and multiplicative structures of the integers.

For our purposes (to connect it to the curves and Mordell) we'd like to remove the dependence on integrality and coprimality, by making it scaling invariant.

We now define

$$H(A, B, C) = \prod_v \max(|A|_v, |B|_v, |C|_v)$$

$$N(A, B, C) = \prod_{p \in I} p$$

for

$$I = \{p \text{ prime} : \max(|A|_p, |B|_p, |C|_p) > \min(|A|_p, |B|_p, |C|_p)\}.$$

Exercise 2.9.4 For sanity.

$$H(\lambda A, \lambda B, \lambda C) = H(A, B, C)$$

$$N(\lambda A, \lambda B, \lambda C) = N(A, B, C)$$

for $\lambda, A, B, C \in \mathbf{Q}^\times$. Moreover if $A, B, C \in \mathbf{Z}$ and gcd = 1 then we recover the original definition.

Since we have $A + B + C = 0$ and our functions are scaling invariant, they only depend on $r = -A/B$. We'll also reformulate it over an arbitrary number field K.

Note that to satisfy the hypotheses of the conjecture we require

$$r \in \mathbf{P}^1_K \setminus \{0, 1, \infty\}.$$

We now define

$$H(r) = \prod_v \max(1, |r|_v)$$

$$N(r) = \prod_{p \in I} p$$

for

$$I = \{p \text{ prime} : \max(v_p(r), v_p(1/r), v_p(r-1)) > 0\}.$$

Remark 2.9.5 In fact this new height is off from the old one by a constant factor, but since ABC allows for a constant factor this won't trouble us.

Motivation: ABC implies Fermat bound. One can see this simply by assuming a solution

$$x^n + y^n = z^n,\ n \geq 3$$

and setting

$$(A, B, C) = (x^n, y^n, z^n)$$

then

$$N(A, B, C) = \prod_{p | ABC} p \leq |xyz| < \max(|x|^3, |y|^3, |z|^3) = H(A, B, C)^{3/n}.$$

So setting

$$\epsilon = 1 - 3/n$$

for (A, B, C) s.t. $H(A, B, C)$ is sufficiently large we get a contradiction to ABC. Thus ABC gives us a bound on the possible solutions to the Fermat equation, reducing the remainder of the conjecture to a finite computation.

Let us phrase this in the following alternate way: Let

$$F_n : x^n + y^n + z^n = 0$$

be the Fermat curve and consider the function

$$f : F_n \longrightarrow \mathbf{P}^1$$

$$(x : y : z) \mapsto -\left(\frac{x}{y}\right)^n$$

ramified over $0, 1, \infty$.

Note 2.9.6 $\deg(f) = n^2$
Each of $0, 1, \infty$ has n preimages in $F_n(\overline{\mathbf{Q}})$.

The idea now is that $N(A, B, C)$ is measuring ramification, while $H(A, B, C)$ is a height function. The note above tells us that each of $0, 1, \infty$ contributes a factor of $O(H(A, B, C)^{n/n^2})$ to $N(A, B, C)$. So in this formulation, what we used was the existence of a rational function f such that

$$\#\{p \in C(\overline{\mathbf{Q}}) : f(p) \in \{0, 1, \infty\}\} < \deg(f).$$

Exercise 2.9.7 If C has genus 0 or 1, no such f can exist (hint: Riemann-Hurwitz).

ABC implies a bound on Mordell. We begin with a technical proposition:

Proposition 2.9.8 *Let K be a number field an d C/K a curve. Let $f \in K(C)$ be a rational function of degree d. Then for $p \in C(K) \setminus f^{-1}(0)$ we have*

$$\log N_0(f(p)) < (1 - b_f(0)/d) \log H(f(p)) + O(\sqrt{\log H(f(p))} + 1)$$

with the following notation

$$N(r) = N_0(r) N_1(r) N_\infty(r)$$

$$N_0(r) = \prod_{\mathfrak{p} \supseteq (r)} \mathrm{Norm}(\mathfrak{p})$$

$$N_1(r) = \prod_{\mathfrak{p} \supseteq (1-r)} \mathrm{Norm}(\mathfrak{p})$$

$$N_\infty(r) = \prod_{\mathfrak{p} \supseteq (1/r)} \mathrm{Norm}(\mathfrak{p})$$

$$b_f(0) = \sum_{f(p)=0} (e_p - 1).$$

Proof. The genus 0 case follows from the fact that the f is a rational function (and in fact the error term is $O(1)$) (exercise). For the general case we need the theory of log heights on curves. From this we require the following

- For D a divisor on C we have a height function

  $$h_D(\cdot)$$

  which is well defined up to $O(1)$.

- If

  $$D = \sum m_k D_k$$

  is a decomposition into irreducible divisors, then

  $$h_D(P) = \sum m_k h_{D_k}(P).$$

- For Δ a degree 0 divisor

  $$h_\Delta(P) = O(\sqrt{\log H(f(P))} + 1).$$

Let $D = \operatorname{div}_0(f) = \sum m_k D_k$, $D' = \sum_{f(P)=0}(P)$ then $b_f(0) = \deg D'$. Then

$$\log H(f(P)) = h_D(P) + O(1) = \sum m_k h_{D_k}(P) + O(1)$$

since $\log H(f(P))$ is also a height function relative to D. We now turn to $N_0(f(P))$. Any prime occurring in this must also occur in $h_{D_k}(P)$ for some k (except for a finite set $\{p : p|f \text{ or } p \text{ bad red. for } C\}$). Then

$$N_0(f(P)) < \sum h_{D_k}(P) + O(1) = h_{D'}(P) + O(1).$$

Letting

$$\Delta = (\deg D)D' - (\deg D')D$$

we have

$$h_\Delta(P) = O(\sqrt{\log H(f(P))} + 1)$$

thus

$$\begin{aligned}\log N_0(f(P)) &< h_{D'}(P) + O(1)\\ &= \frac{1}{\deg D}(\deg D')h_{D'}(P) + O(1)\\ &= \frac{1}{\deg D}(\deg D')h_D(P) + O(\sqrt{\log H(f(P))} + 1)\\ &= \frac{1 - b_f(0)}{d}\log H(f(P)) + O(\sqrt{\log H(f(P))} + 1)\end{aligned}$$

∎

Remark 2.9.9 One can show the above for N_1, N_∞ instead making the appropriate replacements for f.

Adding the three terms together we get

$$\begin{aligned}&\log N_0(f(P))N_1(f(P))N_\infty(f(P))\\ &< \left(\left(1 - \frac{b_f(0)}{d}\right) + \left(1 - \frac{b_f(1)}{d}\right) + \left(1 - \frac{b_f(\infty)}{d}\right)\right)\log H(f(P)) + O(\cdots)\\ \log N(f(P)) &< \frac{1}{d}\left(\#f^{-1}(0) + \#f^{-1}(1) + \#f^{-1}(\infty)\right)\log H(f(P)) + O(\cdots)\\ &< \frac{m}{d}\log H(f(P)) + O(\cdots)\end{aligned}$$

where

$$m = \#\{P \in C(\overline{\mathbf{Q}}) : f(P) \in \{0, 1, \infty\}\}$$

exponentiating we get

$$N(f(P)) < H(f(P))^{m/d}K.$$

Theorem 2.9.10 ABC implies Mordell. *ABC implies Mordell.*

Proof. Let C be a given curve of genus $g \geq 2$ Belyi's theorem gives a function

$$f : C \to \mathbf{P}^1$$

ramified over $\{0, 1, \infty\}$. By Riemann-Hurwitz $m = d + 2 - 2g$, $d = \deg(f)$ m as above. Thus $m < d$, thus we can pick $0 < \epsilon < 1 - \frac{m}{d}$ and so for sufficiently large $H(f(P))$ (i.e. all but finitely many) we have a counterexample to ABC. ∎

Remark 2.9.11 Closing remarks. Belyi's theorem gives an algorithm for determining $f : C \longrightarrow \mathbf{P}^1$ i.e. it is effective.
One can also show ABC implies Siegel's theorem.
In fact it can be shown that a particular effective form of Mordell (applied to $y^2 + y = x^5$) for all number fields implies ABC. This is related to Szpiro's conjecture.

References:

1. Elkies - ABC implies Mordell

2. Serre - Lectures on Mordell-Weil

2.10 Dessins, integer points on elliptic curves and a proof of the ABC conjecture (Alex)

2.10.1 A proof of the ABC theorem (for polynomials)

Last week Angus told us about the incredibly powerful ABC conjecture and its arithmetic consequences (apparently). This week we will prove this conjecture (for polynomials). The proof is very similar to some of the things Angus mentioned, but seeing as I wasn't there its new to me... Following Goldring / Stothers / Parab.

Let K be algebraically closed of characteristic 0, with $f \in K[x]$, we can define the radical as before

$$\operatorname{rad}(f) = \prod_{p|f} p$$

over the primes/irreducibles dividing f, this is the maximal squarefree polynomial dividing f. How do we measure the size of a polynomial? Let $r(f) = \deg \operatorname{rad}(f)$, and $h(f_1, \ldots, f_n) = \max\{\deg f_i\}$. This is a complicated way of saying

$$\#\{x \in K : f(x) = 0\},$$

but we do so to emphasise the link with ABC.

The result is then

Theorem 2.10.1 Mason-Stothers. *Let*

$$e, f, g \in K[x],\ e + f = g$$

be pairwise coprime and all of height > 0. *Then*

$$h(e, f, g) < r(efg) = r(e) + r(f) + r(g).$$

We have sharpness if and only if f/g is a Belyi map for $\mathbf{P}^1 \longrightarrow \mathbf{P}^1$ with $(f/g)(\infty) \in \{0, 1, \infty\}$. Another way of saying this is that if $\deg f = \deg g$ then their leading coefficients are equal, and hence $\deg(e) < \deg(f)$.

Proof. First of all we note that the statement is symmetric in e, f, g, so we may arrange that $h(g) \le h(e, f)$ which implies that $h(e) = h(f) = h(e, f, g)$. The second statement is less obviously invariant but note that ϕ is a Belyi function is equivalent to $1 - \phi$ and $1/\phi$ being Belyi also and this preserves $\phi(\infty) \in \{0, 1, \infty\}$, so rearranging does not change the truth of the second statement either. Let $\phi = f/g$ so $\deg(\phi) = \max\{\deg(f), \deg(g)\} = h(e, f, g)$, we will denote this by h now. Apply Riemann-Hurwitz (suprise-suprise)

$$-2 = -2h + \sum_{x \in \mathbf{P}^1} e_\phi(x) - 1.$$

Let

$$R_y = \sum_{x : f(x) = y} e_\phi(x) - 1$$

be the ramification above y, we will consider B_0, B_1, B_∞. These ramification numbers will simply be $h - \#(\phi^{-1}(y))$. Lets begin with R_1, we have $f(x)/g(x) = 1$ so $e(x) = 0$ and in fact

$$R_1 = h(e) - r(e) = h - r(e).$$

For R_0 we have either $f(x) = 0$ or $g(x) = \infty$. Having $g(x) = \infty$ means $x = \infty$ but this cannot really happen as $h(f) \geq h(g)$. So this is really just

$$\sum_{x : f(x) = 0} e_\phi(x) - 1 = h - r(f).$$

Finally $\phi(x) = \infty$ only when $g(x) = 0$ or $x = \infty$. If $h(f) = h(g)$ then $\phi(\infty) \neq \infty$ and we have simply

$$R_\infty = h - r(g).$$

If $h(g) < h(f)$ then we also have $\phi(\infty) = \infty$ so we pick up an extra preimage and we get instead

$$R_\infty = h - (r(g) + 1).$$

Back up in Riemann-Hurwitz this comes down (magically?) to

$$-2 = \overset{0}{\cancel{-2h + h + h}} + h - r(e) - r(f) - r(g) + R - \delta_{h(f) > h(g)}$$

so

$$R = h - r(efg) - 2 + \delta_{h(f) > h(g)}$$

but of course $R \geq 0$ so

$$h \geq r(efg) + 1$$

with equality exactly when

$$h = r(efg) + 1 \implies R = 0,\ h(f) > h(g).$$

$R = 0$ is equivalent to being Belyi. ■

2.10.2 Back to number theory

That was all well and good, but this is a number theory seminar, not a function field analogues of number theory seminar, so let's take it back to why we are all here, solving Diophantine equations.

Let's try and find nontrivial integral points on Mordell curves!

$$E_k : y^2 = x^3 + k.$$

Example 2.10.2

$$1001^2 = 5009^3 - (5009^3 - 1001^2)$$

so I found a large point on

$$y^2 = x^3 - (5009^3 - 1001^2) = x^3 - 125675213728$$

are you not impressed? □

Although this point would look slightly non-trivial if I started with the curve 5009^3 is roughly 125675213728 anyway so you should only be impressed if I find points of height somewhat larger than the coefficients. We should probably ask that

$$|x|^3 > |k|$$

by some margin at least.

A nice question is then given k how big can an integer point (x, y) on E_k be? Bounds are known, e.g. Via work of Baker we get

$$\max(|x|, |y|) < e^{10^{10}|k|^{1000}}.$$

Ouch.

If we want to study more realistic bounds we can instead reverse the problem. Can we minimise $x^3 - y^2$ for integer x, y, how close can the square of a large integer and the cube of a large integer be? Euler showed that $|x^3 - y^2| = 1$ has only 1 (interesting) solution, for example.

Marshall Hall was interested in this, did some nice computations and conjectured:

Conjecture 2.10.3 Mashall Hall's conjecture, 1970. *If*

$$x^3 - y^2 = k$$

for integers x, y then

$$|k| > \frac{\sqrt{|x|}}{5}$$

(or $k = 0$...).

This is false!

Example 2.10.4 Elkies (who else?). If

$$x = 5853886516781223, \; y = 447884928428402042307918$$

is a point on

$$y^2 = x^3 - 1641843$$

then

$$\frac{\sqrt{|x|}}{k} = 46.6004943471754.$$

□

This is far larger than the previous best known, but still remains the record as far as I can tell. It seems Hall's conjecture is unlikely to be true for any fixed constant, but the following of Stark-Trotter is more believable.

Conjecture 2.10.5 Stark-Trotter/Weak Hall. *For any $\epsilon > 0$ there is some $C(\epsilon)$ such that for any x, y integers*

$$|x^3 - y^2| > C(\epsilon)x^{\frac{1}{2}-\epsilon}$$

for any $x > C(\epsilon)$.

If Hall's/Stark-Trotter is true we get a *huge* improvement on Baker

$$\frac{\sqrt{|x|}}{|k|} < 100 \implies x < 10^4 k^2$$

and hence

$$y^2 = x^3 + k < 10^{12} k^6 + k$$

giving polynomial bounds on x, y in terms of k.

How might one find such triple (x, y, k) that is extremal? One approach is to try and come up with a parametrisation of nice triples. We can search for polynomials $X(t), Y(t), K(t)$ and then plug in various integer values for t and hope for the best. To give ourselves the best chance of succeeding we want $K(t)$ to be smaller than $X(t)^3$ and $Y(t)^2$ for some values of t. This leads us to ask for K to be of smallest degree possible. So how low can we go?

This is the point where we come full circle right, we are searching for

$$X(t)^3 - Y(t)^2 = K(t)$$

with degree of K minimised, so we apply Mason-Stothers to see that, if M is the degree of the left hand terms we have $\deg(X) = 2m$ and $\deg(Y) = 3m$, indeed h in Mason-Stothers is then $6m$ We also have $r(X^3) = r(X) \leq 2m$ and $r(X^2) = r(Y) \leq 3m$ so together Mason-Stothers gives

$$6m < 2m + 3m + r(K)$$

or $m < r(K)$. So we have lower-bounded the degree of K in terms of $\frac{1}{2}\deg(X)$ for example.

We just proved:

Conjecture 2.10.6 Birch B. J., Chowla S., Hall M., Jr., Schinzel A. On the difference $x^3 - y^2$, 1965.. *Let X, Y be two coprime polynomials with X^3, Y^2 of equal degree $(6m)$ and equal leading coefficient, then*

$$K = X^3 - Y^2$$

is of degree $> m$.
(Now the speaker has just given a theorem with an inequality, so in order to appear smart one of you should ask is this bound sharp.)
The bound is sharp, this can mean several things in general, originally it was asked that for infinity many m there is an example where $\deg K = m + 1$.

The first part was proved initially by Davenport (in the same year, and journal). The second part had to wait until '81 for Stothers to prove it.

Someone else should probably also ask, how is any of this related to Dessins?

To prove sharpness we have to exhibit for each m triple of polynomials X, Y, K of degrees $2m, 3m, m+1$. Coming up with polynomial families is hard, drawing stupid pictures is easy, can Dessins aid us here?

Lets back-track, when we proved Mason-Stothers we also said that sharpness was equivalent to f/g being Belyi, so $X(t)^3/K(t) = (K(t) + Y(t)^2)/K(t) = Y(t)^2/K(t)+1$ should be a Belyi map of degree $6m$ from $\mathbf{P}^1 \to \mathbf{P}^1$. What does its ramification look like? We should have all preimages of 0 degree 3, preimages of 1 degree 2, and above infinity $m + 1$ points of degree 1 and the remaining of degree $6m - (m + 1) = 5m - 1$.

How can we draw a Dessin like this? Begin with a tree with all internal vertices degree 3, with $2m$ vertices, this will have $2m - 1$ edges, and as it is trivalent by the handshake lemma

$$3\#\{\text{internal}\} + \#\{\text{leaves}\} = 4m - 2$$

and

$$\#\{\text{internal}\} + \#\{\text{leaves}\} = 2m$$

giving

$$2\#\{\text{internal}\} = 2m - 2$$
$$\#\{\text{internal}\} = m - 1$$
$$\#\{\text{leaves}\} = m + 1$$

Add loops to the leaves, you now have a clean Dessin as above. It has $2m-1+m+1 = 3m$ edges. We have a face for every loop of degree 1, and one on the outside of degree $m+1+2(2m-1) = 5m-1$ as each internal edge is traversed twice if you walk around the outside. So this works!

Example 2.10.7 For $m = 1$

$$(x^2+2)^3 - (x^3+3x)^2 = 3x^2 + 8.$$

$m = 2$

$$(x^4-4x)^3 - (x^6-6x^3+6)^2 = 8x^3 - 36.$$

□

Example 2.10.8 For $m = 5$

$$X(t) = \frac{1}{9}(t^{10} + 6t^7 + 15t^4 + 12t)$$

$$Y(t) = \frac{1}{54}(2t^{15} + 18t^{12} + 72t^9 + 144t^6 + 135t^3 + 27)$$

$$K(t) = -\frac{1}{108}(3t^6 + 14t^3 + 27)$$

and we can let $t = -3$ to get $X(-3) = 5234$, $Y(-3) = -378661$ and $K(-3) = -17$, so we have a point

$$(5234, 378661) \in E_{17} \colon y^2 = x^3 + 17$$

letting $t = \pm 9$ we get

$$|384242766^3 - 7531969451458^2| = 14668$$

$$|390620082^3 - 7720258643465^2| = 14857$$

both of which have

$$\frac{\sqrt{|x|}}{k} \approx 1.33,$$

these get lower as we increase t though. □

We should expect this decrease from this method as if $\deg X = 2m$ and $\deg K = m+1$ then $\sqrt{X(t)}/K(t)$ grows like $t^m/t^{m+1} = t^{-1}$.

Can we do the same for abc?

Take the Dessin with a deg 1 vertex at infinity, degree 3 at 0 with an edge surrounding 1, we get a Belyi function

$$f(x) = \frac{64x^3}{(x+9)^3(x+1)}, \; f(x) - 1 = -\frac{(x^2-18x-27)^2}{(x+9)^3(x+1)}$$

plugging in $x = a/b$ and cross multiplying gives

$$64a^3b + (a^2 - 18ab - 27b^2)^2 = (a+9b)^3(a+b)$$

which could of course be verified independently, but how would you find this identity without Dessins? Now for $a = -32, b = 23$ we get

$$-2^{21} \cdot 23 + 11^2 = -1 \cdot 3^2 \cdot 5^6 \cdot 7^3$$

or

$$11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$$

This is the second highest quality abc triple known with quality

$$\frac{\log c}{\log R} = 1.62599$$

(the current winner has quality 1.6299).

References. A semi-random order, maybe starting at the top is nice though. If you have trouble finding something let me know.

1. On Computing Belyi Maps - J. Sijsling, J. Voight
2. Belyi Functions: Examples, Properties, and Applications - Zvonkin (really nice survey)
3. On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's Existence Theorem - Umberto Zannier
4. Unifying Themes Suggested by Belyi's Theorem - Wushi Goldring
5. Polynomial Identities and Hauptmoduln - W. W. Stothers
6. Elliptic Surfaces and Davenport-Stothers Triples - Tetsuji Shioda
7. The abc-theorem, Davenport's inequality and elliptic surfaces - Tetsuji Shioda
8. It's As Easy As abc - Andrew Granville, Thomas J. Tucker
9. Polynomial and Fermat-Pell families that attain the Davenport-Mason bound - Noam D. Elkies, Mark Watkins (on Watkins webpage)
10. Halltripels en kindertekeningen - Hans Montanus (in Dutch, but math is universal right?)
11. Computational Number Theory and Algebraic Geometry Spring 2012, taught by Noam Elkies, notes by Jason Bland
12. Davenport-Zannier polynomials over **Q** - Fedor Pakovich, Alexander K. Zvonkin (a nice extension perhaps?)
13. Minimum Degree of the Difference of Two Polynomials over Q, and Weighted Plane Trees - Fedor Pakovich, Alexander K. Zvonkin (as above)
14. The ABC-conjecture for polynomials - Abhishek Parab
15. On Marshall Hall's Conjecture and Gaps Between Integer Points on Mordell Elliptic Curves - Ryan D'Mello

16. Neighboring powers - F. Beukers, C. L. Stewart (a more general problem, but nice history and examples)
17. Rational Points Near Curves and Small Nonzero $|x^3 - y^2|$ via Lattice Reduction - Elkies
18. ABC implies Mordell - Elkies
19. Dessins d'enfant - Jeroen Sijsling (master thesis)
20. Algorithms and differential relations for Belyi functions - Mark van Hoeij, Raimundas Vidunas.
21. Belyi functions for hyperbolic hypergeometric-to-Heun transformations - Mark van Hoeij, Raimundas Vidunas (has application to ABC over number fields at the end)
22. Some remarks on the S-unit equation in function fields - Umberto Zannier
23. A note on integral points on elliptic curves - Mark Watkins
24. On Hall's conjecture - Andrej Dujella (more recent progress)
25. Hecke Groups, Dessins d'Enfants and the Archimedean Solids - Yang-Hui He, and James Read
26. Belyi functions for Archimedean solids - Nicolas Magot, Alexander Zvonkin (didn't really use this but it's nice!)

2.11 Three Short Stories about Belyi's theorem (Ricky)

Theorem 2.11.1 $X/\mathbf{C}$ *a curve. Then* X *is defined over* $\overline{\mathbf{Q}}$ *iff there exists a Belyi map*

$$\phi \colon X \to \mathbf{P}^1$$

such that $B(\phi) \subseteq \{0, 1, \infty\}$.

Main reference: Unifying Themes Suggested by Belyi's Theorem - Wushi Goldring

2.11.1 The case of the Rising Degree

Definition 2.11.2 The **Belyi degree** of $X/\overline{\mathbf{Q}}$ (a curve) is the minimal degree of $\phi \colon X \to \mathbf{P}^1$ a Belyi map. ◊

Question, how does the Belyi degree of $X/\overline{\mathbf{Q}}$ relate to the arithmetic of X?

Definition 2.11.3 The **field of moduli** of $X/\overline{\mathbf{Q}}$ is the intersection over all fields $\subseteq \overline{\mathbf{Q}}$ over which X is defined. Similarly for a morphism $\phi \colon X \to Y$. ◊

Remark 2.11.4 This is not the same as the field of definition always.

Given $X/\overline{\mathbf{Q}}$ with field of moduli K we say X has good (resp. semistable) reduction at $\mathfrak{p} \subseteq O_K$ if there exists a model for X over $O_{K_\mathfrak{p}}$ s.t. the special fibre is smooth (resp. semistable) reduction.

For $p \in \mathbf{Z}$ we say X has good/semistable reduction at p if it dies for all $\mathfrak{p} | p$.

Theorem 2.11.5 Zapponi. *If $X/\overline{\mathbf{Q}}$ then the Belyi degree of X is at least the largest prime $p \in \mathbf{Z}$ such that X has bad semistable reduction at p.*

Remark 2.11.6

1. The lower bound is not "sharp" because there exist E/K with good reduction everywhere, but no degree 1 maps $\phi\colon E \longrightarrow \mathbf{P}^1$.

2. If
$$E\colon y^2 = x^3 + x^2 + p$$
then E has bad semistable reduction at p so the Belyi degree of E is $\geq p$.

Theorem 2.11.7 Beckmann. *Let $\phi\colon X \longrightarrow \mathbf{P}^1$ be a Belyi map with field of moduli M. Let G be the Galois group of the Galois closure of ϕ. Then for all p such that $p \nmid |G|$, $\tilde{\phi}\colon \tilde{X} \longrightarrow \mathbf{P}^1$ has good reduction at p and p is unramified in M.*

Proof. Of Zapponi.
Let $\phi\colon X \longrightarrow \mathbf{P}^1$ be a Belyi map of degree n. Let K be the field of moduli of X, M the field of moduli of ϕ then M/K is a finite extension. Take G as above and let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a place of bad semistable reduction for X. Then $\wp|\mathfrak{p}$ for $\wp \subseteq \mathcal{O}_M$ is a place of bad semistable reduction for ϕ. By Theorem 2.11.7 $p \mid |G|$ for $p \in \mathbf{Z}$ below $\mathfrak{p}$ but $G \hookrightarrow S_n$ which implies $p|n!$ so $p \leq n$. ∎

2.11.2 Finitists Dream

Recall that if k is a perfect field of characteristic p then
$$\phi\colon C_1 \to C_2$$
is said to be tamely ramified at $P \in C_1$ if $p \nmid e_\phi(P)$ (wildly ramified if $p|e_\phi(P)$).

Theorem 2.11.8 Wild p-Belyi. *For C a curve over k perfect of characteristic p, there exists a "wild Belyi map"*
$$\phi\colon C \to \mathbf{P}^1$$
such that $B(\phi) = \{\infty\}$. I.e. every curve $/k$ is birational to an étale cover of $\mathbf{A}^1$.

Example 2.11.9
$$\mathbf{G}_m \to \mathbf{A}^1$$
$$x \mapsto x^p + \frac{1}{x}$$
but the tame étale fundamental group of $\mathbf{A}^1$ is 0. □

Theorem 2.11.10 Tame p-Belyi (Saidi). *Let $p > 2$. For $C/\overline{\mathbf{F}}_p$ there exists $\phi\colon C \to \mathbf{P}^1$ tamely ramified everywhere (i.e. possibly unramified) with*
$$B(\phi) \subseteq \{0, 1, \infty\}.$$

Lemma 2.11.11 Fulton. *Let $p > 2$ then for C/k (k algebraically closed of characteristic p) there exists $\psi\colon C \longrightarrow \mathbf{P}^1$ such that*
$$e_\psi(P) \leq 2.$$

Proof. Of Tame p-Belyi
Take $\psi\colon C \longrightarrow \mathbf{P}^1$ as in the lemma then
$$B(\psi) \subseteq \mathbf{P}^1(\mathbf{F}_{p^m})$$

for some m. Define

$$f\colon \mathbf{P}^1 \to \mathbf{P}^1$$

by

$$x \mapsto x^{p^m-1}.$$

Take $\phi = f \circ \psi$. So π is tamely ramified everywhere and $B(\phi) \subseteq \{0, 1, \infty\}$. ■

Analogue of Fulton's lemma is that there exists

$$\tau : C \to \mathbf{P}^1$$

for $\mathrm{char}(k) \neq 3$ such that $e_\tau(P) = 1$ or 3.

2.11.3 In the Stacks

Observation 2.11.12 $\mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$ is the moduli space of genus 0 curves with four (ordered) marked points.

$$(\mathbf{P}^1, \alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto \mathrm{im}(\alpha_4) \text{ when } \alpha_1 \mapsto 0, \alpha_2 \mapsto 1, \alpha_3 \mapsto \infty.$$

Definition 2.11.13 Let $\mathcal{M}_{g,n}$ be the moduli space of genus g curves with n (ordered) marked points (then $\mathcal{M}_{g,[n]}$ is the same for unordered points). If n is large enough relative to g then $\mathcal{M}_{g,n}$ will be a scheme (but the unordered version will not). ◊

Example 2.11.14

$$\mathcal{M}_{0,4} \simeq \mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$$

□

Question 2.11.15 Braungardt. Is every $X/\overline{\mathbf{Q}}$ (smooth projective variety) birational to a finite étale cover of some $\mathcal{M}_{g,[n]}$? □

Note 2.11.16 There exists an étale map

$$\mathcal{M}_{g,n} \to \mathcal{M}_{g,[n]}$$

by forgetting the ordering of the points.

So the dimension 1 case of the conjecture is Belyi's theorem, by

$$X \smallsetminus \phi^{-1}(B(\phi)) \to \mathbf{P}^1 \smallsetminus \{0, 1, \infty\} \simeq \mathcal{M}_{0,4} \to \mathcal{M}_{0,[4]}.$$

In dimension 2 we have $\mathcal{M}_{1,[2]}$ and $\mathcal{M}_{0,[5]}$, the only 2-d spaces of interest. We also have an étale map

$$\mathcal{M}_{1,[2]} \xrightarrow{\alpha} \mathcal{M}_{0,[5]}$$

as follows:

$$\eta = (E; \{q_1, q_2\}) \in \mathcal{M}_{1,[2]}$$

with

$$\alpha(\eta) = (\mathbf{P}^1; \{r_1, r_2, r_3, r_4, r_5\})$$

where the r_i come from constructing a projection ϕ from E to $\mathbf{P}^1$ situated perpendicularly to the line joining q_1, q_2. This then has 4 ramification points

$$B(\phi) = \{r_1, r_2, r_3, r_4\}$$

and $r_5 = \phi(q_1) = \phi(q_2)$. So Braungardt for surfaces $(X/\overline{\mathbf{Q}})$? Does there exist $\phi\colon X \to \mathcal{M}_{0,[5]}$ which is étale?

Theorem 2.11.17 Braungardt. *For $X/\overline{\mathbf{Q}}$ an abelian surface X is birational to an étale cover of $\mathcal{M}_{0,[5]}$.*

Proof. Sketch.

For an abelian surface over $\overline{\mathbf{Q}}$ there exists another isogenous to it which is principally polarized. Such surfaces come in two flavours

$$E_1 \times E_2$$

or $J(C)$ for C of genus 2.

Case 1:

Let $\phi_i \colon E_i \to \mathbf{P}^1 \setminus \{0,1,\infty\}$ be Belyi maps. Then we have $\alpha \colon A \xrightarrow{\phi_1,\phi_2} \mathbf{P}^1 \times \mathbf{P}^1$. Then α restricts to a finite unramified cover

$$\alpha^{-1}(S) \xrightarrow{\alpha} S$$

where

$$S = (\mathbf{P}^1 \setminus \{0,1,\infty\} \times \mathbf{P}^1 \setminus \{0,1,\infty\}) \setminus \Delta.$$

Note that $S \simeq \mathcal{M}_{0,5}$ by

$$(a,b) \mapsto (\mathbf{P}^1; \{0,1,\infty,a,b\}).$$

So A is birational to $\alpha^{-1}(S)$ which is an étale cover of $\mathcal{M}_{0,[5]}$.

Case 2

If $A = J(C)$ then use $\phi \colon C \to \mathbf{P}^1$ and a relation between A and $\mathrm{Sym}^2(C)$. ∎

2.12 Dessins in Physics (Jim)

Physics. Let M be a manifold with a metric g. We call the pair (M,g) a "spacetime manifold". Let $\mathcal{E}$ be a "space of fields", either $C^\infty(M)$, sections of some $E \to M$, connections, or similar.

$$S(\phi) = \int_M \mathcal{L}(\phi)$$

for $\phi \in \mathcal{E}$ and $\mathcal{L}$ the Lagrangian. "Physically realisable states" are then fields ϕ that minimise $S(\phi)$. W is a superpotential, this is a term in $\mathcal{L}$ that satisfies some special symmetries. E.g. we could also have

$$S(\phi_1,\phi_2) = \int_M \mathcal{L}(\phi_1,\phi_2)$$

the W might satisfy $W(\phi_1,\phi_2) = W(\phi_2,\phi_1)$.

Definition 2.12.1 Gauge transformations. Let $G \circlearrowright E \xrightarrow{p} M$ be an action s.t. each fibre $E_x = p^{-1}(x)$ is a representation of G. A **gauge** is a section $s(x)$ of $E \to M$. A **gauge transformation** is a map $g \colon M \to G$ s.t.

$$g(x)s(x)$$

is another section, call G the **gauge group**. The important gauge transformations are the ones that fix the set of physically realisable states (i.e. fixes the subset of $\mathcal{E}$ that minimise S). ◊

Quivers and dessins. Let's now study the relationship between quivers and dessins.

Example 2.12.2 $\mathcal{N} = 4$ SYM (supersymmetric Yang-Mills) (Gauge symmetries given by some product of $SU(N)$) . □

A quiver is a directed graph, possibly with self-loops. Here we think of the nodes as corresponding to factors of the gauge group. And the arrows as fields, so in a bouquet with 3 petals we have three fields, and only $G = SU(N)$.

There is also the notion of a periodic quiver (a tiling of the plane). We can take the triangular lattice and consider its dual, this is a hexagonal tiling with a bicolouring corresponding to the fact we had upwards pointing and downwards pointing triangles. This is a Dimer model.

Relating the Dimer model back to physics: We have hexagonal faces in correspondence with factors of the Gauge group, and edges fields, with vertices terms in W.

So one distinct face gives one factor in the gauge group so $G = SU(N)$. 3 distinct edges give 3 fields X_1, X_2, X_3. To recover W consider the permutation arising from reading the edges around the vertices counterclockwise. A black vertex $(1, 2, 3)$ gives σ_B corresponding to a positive term in W. A white vertex $(1, 2, 3)$ gives σ_W corresponding to a negative term in W. Then $\sigma_\infty = (\sigma_B \sigma_W)^{-1} = (123)$ σ_i gives a term for each cycle. Each cycle in σ_B gives a product of fields indexed by the cycle, e.g. in this example σ_B gives $X_1X_2X_3$. Each cycle in σ_W^{-1} gives a product of fields indexed by the cycle, e.g. in this example σ_W gives $X_1X_3X_2$. Then

$$\begin{aligned} W &= \mathrm{Tr}((\text{sim of } \sigma_B \text{ terms}) - (\text{sim of } \sigma_W \text{ terms})) \\ &= \mathrm{Tr}(X_1X_2X_3 - X_1X_3X_2). \end{aligned}$$

$$\begin{aligned} \mathrm{Aut}(\{\sigma_B, \sigma_W, \sigma_\infty\}) &= \{\gamma \in S_3 : \gamma\sigma_i\gamma^{-1} = \sigma_i) \\ &= \{1, (123), (132)\} \\ &= \mathbf{Z}/3\mathbf{Z}. \end{aligned}$$

The fundamental domain of the Dimer gives a dessin on the torus with two vertices of degree 3. This corresponds to the Belyi pair (Σ, β) where

$$\Sigma\colon y^2 = x^3 + 1$$

$$\beta\colon \Sigma \longrightarrow \mathbf{P}^1$$

$$(x, y) \mapsto \frac{y+1}{2}.$$

$$\mathrm{Aut}(\Sigma, \beta) \simeq \mathrm{Aut}(\{\sigma_B, \sigma_W, \sigma_\infty\})$$

$\mathrm{Aut}(\Sigma, \beta)$ is generated by

$$(x, y) \mapsto (w^3x, y)$$

where $w^3 = 1$.

Example 2.12.3 Take the quiver with two vertices and two edges in each direction connecting them. This has 4 fields and two factors of G (i.e. $G = SU(N) \times SU(N)$). The dimer is a square lattice alternately coloured, with $\sigma_B = \sigma_W = (1234)$, $\sigma_\infty = (13)(24)$.

$$W = \mathrm{Tr}(X_1X_2X_3X_4 - X_1X_4X_3X_2).$$

In this case the Belyi pair is

$$\Sigma\colon y^2 = x(x-1)(x-\frac{1}{2})$$

$$\beta = \frac{x^2}{2x-1}.$$
$$\mathrm{Aut}(\{\sigma_B, \sigma_W, \sigma_\infty\}) = \langle(1234)\rangle \simeq \mathbf{Z}/4\mathbf{Z}$$
$$\phi_\pm \colon (x,y) \mapsto \left(\frac{x}{2x-1}, \frac{\pm i}{(2x-1)^2}\right)$$
$$\phi_+^2 = \phi_-^2 \colon (x,y) \mapsto (x,-y)$$
$$\phi_+^3 = \phi_+^{-1} = \phi_-$$
$$\phi_+^4 = 1$$

so

$$\mathrm{Aut}(\Sigma, \beta) \simeq \mathbf{Z}/4\mathbf{Z}$$
$$\beta^{-1}(0) = \{(0,0)\}$$
$$\beta^{-1}(1) = \{(1,0)\}$$
$$\beta^{-1}(\infty) = \{(\frac{1}{2},0), (\infty,\infty)\}$$

on the Dimer we have the square lattice so taking a fundamental domain containing of the vertices we see the torus as a topology. □

Example 2.12.4 Final example. Let's jump straight to the Dimer the hexagonal lattice with fundamental domain containing 6 vertices. We have 9 fields and three factors in the gauge group $G = \mathrm{SU}(N)^2$.

$$\sigma_B = (147)(258)(369)$$
$$\sigma_W = (123)(456)(789)$$
$$\sigma_\infty = (195)(276)(384)$$

so

$$W = \mathrm{Tr} \sum_{i,j,k} X_{12}^i X_{23}^j X_{31}^k \epsilon_{ijk}$$

where

$$\epsilon_{ijk} = \begin{cases} \mathrm{sgn}(ijk) & \text{if } i,j,k \text{ distinct} \\ 0 & \text{otw} \end{cases}$$

X_{12}^i acts on the ith field by $N, \bar{N}, 1$ where N is the canonical representation, $\bar{N}$ the anticanonical and 1 is trivial.

$$\mathrm{Aut}(\{\sigma_B, \sigma_W, \sigma_\infty\}) \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$$

now the Belyi pair

$$\Sigma = \text{projective closure of } F = \{(x,y) : x^3 + y^3 = 1\}$$
$$\beta(x,y) = x^3$$
$$\gamma_1(x,y) = (w_1 x, y)$$
$$\gamma_2(x,y) = (x, w_2 y)$$
$$w_i^3 = 1.$$

□

Chapter 3

Supersingular isogeny graphs and Quaternion Algebras

These are notes for BUNTES Fall 2018, the topic is Supersingular isogeny graphs and Quaternion Algebras.

http://math.bu.edu/people/midff/buntes/fall2018.html.

Outline:

1. Background, isogeny graphs, applications.
2. Supersingular isogeny graph cryptography (candidate for post-quantum cryptography).
3. Introduction to Quaternion algebras.
4. The Deuring correspondence:

$$\left\{\text{maximal orders } \mathcal{O} \subseteq B_{p,\infty}\right\} /\sim \leftrightarrow \left\{j \text{ s.s. } \in \mathbf{F}_{p^2}\right\} /\mathrm{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p).$$

References: [66, 72, 71]

3.1 Isogeny graphs: background and motivation (Maria Ines)

3.1.1 Background

Let $k = \mathbf{F}_q$, $\mathrm{char}(k) = p \neq 2, 3$.

Definition 3.1.1 Elliptic curves. An **elliptic curve** E/k is a smooth projective curve of genus 1 together with a point $\infty \in E(k)$. $\Diamond$

We can always write such a curve using a Weierstrass equation

$$E\colon y^2 = x^3 + ax + b,\ a, b \in k$$

E is really the projective closure of this affine equation.

Definition 3.1.2 j-invariants. The j-invariant of an elliptic curve E is

$$j(E) = j(a, b) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

doesn't depend on the choice of Weierstrass equation. $\Diamond$

Fact 3.1.3

1. *E, E' are isomorphic over $\overline{k} \iff j(E) = j(E')$.*
2. *There is a 1-1 correspondence*

$$k \leftrightarrow \overline{k}\text{-isomorphism classes of EC's }/k.$$

Definition 3.1.4 Isogenies. Let $E, E'/k$ be elliptic curves. An **isogeny**, $\phi \colon E \to E'$ is a non-constant morphism of pointed curves. The degree $\deg \phi$ is the degree as a morphism. E, E' are said to be n-isogenous if there exists $\phi \colon E \to E'$ of degree n. $j, j' \in k$ are n-isogenous if the corresponding elliptic curves are.◊

Fact 3.1.5

1. *If $p \nmid n = \deg \phi$ then the kernel of ϕ has size n (ϕ is separable).*
2. *every finite subgoup of $E(\overline{k})$ is the kernel of a separable isogeny from E, unique up to isomorphism.*
3. *Every n-isogeny $\phi \colon E \to E'$ has a dual isogeny $\hat{\phi} \colon E' \to E$ such that*

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [n],$$

   the multiplication-by-n map.

4. *The n-torsion subgroup*

$$E[n] = \left\{P \in E(\overline{k}) : nP = \infty\right\}$$

   is isomorphic to $(\mathbf{Z}/n)^2$ if $p \nmid n$.

Lemma 3.1.6 *Let E/k be an elliptic curve with $j(E) \notin \{0, 1728\}$ and let $l \neq p$ be prime, up to isomorphism the number of l-isogenies from E defined over k is 0,1,2 or $l + 1$.*

Proof. In Maria's notes. ∎

The modular equation. Let $j(\tau)$ be the modular j-function. For each prime l the minimal polynomial ϕ_l of $j(l\tau)$ over $\mathbf{C}(j(\tau))$ is the modular polynomial

$$\phi_l \in \mathbf{Z}[j(\tau)][y] \simeq \mathbf{Z}[x, y].$$

Fact 3.1.7

1. *ϕ_l is symmetric in x, y and has a degree $l + 1$ in both variables.*
2. *The modular equation*

$$\phi_l(x, y) = 0$$

   is a canonical model for

$$Y_0(l) = \Gamma_0(l)\backslash\mathbf{H}$$

   it parameterises pairs of elliptic curves related by an l-isogeny. This moduli interpretation is still valid when we use any field F with $\mathrm{char}(F) \neq l$.

3. *Let $m_l(j, j') = \mathrm{ord}_{t=j'}\, \phi_l(j, t)$, whenever $j, j' \neq 0, 1728$,*

$$m_l(j, j') = m_l(j', j).$$

The endomorphism ring.

Definition 3.1.8 Endomorphisms of elliptic curves. An **endomorphism** of an elliptic curve E is either the zero map or an isogeny from E to itself. They form a ring $\mathrm{End}(E)$. ◊

For $n \in ZZ$ we ahve $[n] \in \mathrm{End}(E)$ so $\mathbf{Z} \subseteq \mathrm{End}(E)$ over a finite field k, $\mathrm{End}(E)$ is always larger than $\mathbf{Z}$. It is either an order in an imaginary quadratic field, in which case we say E is ordinary. Or an order in an quaternion algebra, in which case we say E is supersingular. We say E has complex multiplication by $\mathcal{O}$.

Proposition 3.1.9 *Let $E/k = \mathbf{F}_{p^n}$ be an elliptic curve, TFAE*

1. *E is supersingular.*
2. *$E[p]$ is trivial.*
3. *The map $[p]\colon E \to E$ is purely inseparable and $j(E) \in \mathbf{F}_{p^2}$.*

Note 3.1.10 If E, E' are isogenous elliptic curves then $\mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q} \simeq \mathrm{End}(E') \otimes_{\mathbf{Z}} \mathbf{Q}$. So supersingularity is preserved by isogenies.

Isogeny graphs of elliptic curves. Let $k = \mathbf{F}_q$ with $\mathrm{char}(k) = p$ and $l \neq p$ be prime.

Definition 3.1.11 Isogeny graphs. The l-isogeny graph $G_l(k)$ is the directed graph with vertex set k and edges (j, j') present with multiplicity

$$m_j(l, l') = \mathrm{ord}_{t=j}\, \phi_l(j, t)$$

vertices are $\overline{k}$ isomorphism classes of elliptic curves $/k$, edges are isomorphism classes of l-isogenies defined over k. ◊

Since $m_l(j, j') = m(j', j)$ whenever $j, j' \neq 0, 1728$ the subgraph of $G_l(k)$ supported on $k \setminus \{0, 1728\}$ can be thought of as undirected. By the last note $G_l(k)$ consists of ordinary and supersingular components.

Supersingular isogeny graphs. Since every supersingular j-invariant lives in $\mathbf{F}_{p^2}$ if E is supersingular all roots of $\phi_l(j(E), y)$ live in $\mathbf{F}_{p^2}$. Every vertex in a supersingular component has out-degree $l + 1$.

Moreover by a result of Kohel $G_l(\mathbf{F}_{p^2})$ has only one supersingular component.

By the above if $p \equiv 1 \pmod{12}$ then the supersingular component of $G_l(\mathbf{F}_{p^2})$ is an undirected $(l+1)$-regular graph with around $p/12$ vertices.

Theorem 3.1.12 Pizer. *The supersingular component of $G_l(\mathbf{F}_{p^2})$ is a Ramanujan graph.*

Definition 3.1.13 Ramanujan graphs. A connected d-regular graph is a **Ramanujan graph** if $\lambda_2 \leq \sqrt{d-1}$ where λ_2 is the second largest eigenvalue of its adjacent matrix. (The largest one is always d, by d-regularity.) ◊

Ordinary isogeny graphs. Let $E/\mathbf{F}_q$ be an ordinary elliptic curve, then $\mathrm{End}(E) \simeq \mathcal{O}$ is an order in an imaginary quadratic field K with $\mathbf{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ where π is Frobenius and

$$K = \mathbf{Q}(\sqrt{(\mathrm{Tr}\,\pi)^2 - 4q})$$

by Tate, isogenous elliptic curves have the same $\mathrm{Tr}\,\pi$.

We can separate the vertices in the component V of $G_l(k)$ containing $j(E)$ into levels $V_0, \dots, V_d$ so that $j(E') \in V_i$ if $i = v_l([\mathcal{O}_K : \mathcal{O}'])$. We'll see that $\bigcup_{i=0}^d V_i$ is connected.

Let $\phi\colon E \longrightarrow E'$ be an l-isogeny between two elliptic curves with CM by $\mathcal{O} = \mathbf{Z} + \tau\mathbf{Z}$, $\mathcal{O}' = \mathbf{Z} + \tau'\mathbf{Z}$. Then $\hat{\phi}\tau'\phi \in \mathrm{End}(E) \implies l\tau' \in \mathcal{O}$. Similarly $l\tau \in \mathcal{O}'$. There are 3 cases

1. $\mathcal{O} = \mathcal{O}'$ (ϕ is horizontal).
2. $[\mathcal{O} : \mathcal{O}'] = l$ (ϕ is descending).
3. $[\mathcal{O}' : \mathcal{O}] = l$ (ϕ is ascending).

In the last two cases we say ϕ is critical.

Horizontal isogenies. E/k with CM by $\mathcal{O} \subseteq K$ imaginary quadratic. Let $\mathfrak{a}$ be an invertible ideal.

$$E[\mathfrak{a}] = \{P \in E(\overline{k}) : \alpha(P) = 0\,\forall \alpha \in \mathfrak{a}\}$$

this is a finite group so it is the kernel of a separable isogeny $\phi_{\mathfrak{a}}$. If $p \nmid N(\mathfrak{a})$ then $\deg(\phi_{\mathfrak{a}}) = N(\mathfrak{a})$ with $\mathfrak{a}$ invertible implying $\phi_{\mathfrak{a}}$ is horizontal.

Each horizontal l-isogeny ϕ arises from some invertible ideal $\mathfrak{a}$ of norm l.

If $l | [\mathcal{O}_K : \mathcal{O}]$ no such ideals exist, otherwise the number of invertible ideals of norm l is

$$1 + \left(\frac{\mathrm{disc}(K)}{l}\right) = \begin{cases} 0 & \text{if } l \text{ inert} \\ 1 & \text{if } l \text{ ramified} \\ 2 & \text{if } l \text{ splits} \end{cases}$$

Vertical isogenies. Let $\mathcal{O}$ be an order in an imaginary quadratic field K of discriminant $D < -4$ and let $\mathcal{O}' = \mathbf{Z} + l\mathcal{O}$.

Lemma 3.1.14 *Let E'/k be an elliptic curve with CM by $\mathcal{O}'$ then there is a unique ascending l-isogeny $E' \longrightarrow E$ with E/k an elliptic curve with CM by $\mathcal{O}$.*

Definition 3.1.15 An l-volcano V is a connected undirected graph whose vertices are partitioned into levels $V_0, \dots, V_d$.

1. The subgraph V_0 is regular of degree ≤ 2.
2. For each $i > 0$ each vertex in V_i has exactly one neighbour in level V_{i-1}, and this accounts for all edges outside of V_0.
3. For $i < d$ each vertex has degree $l + 1$.

The number d is the depth. ◊

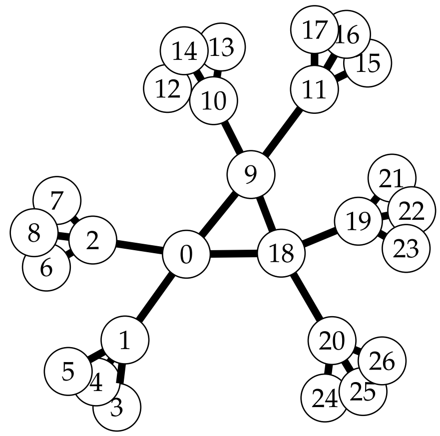

Figure 3.1.16: A 3-volcano

The Sage code used to make this picture was:

```
N = 3 # number of flows
p = 3
d = 2
G = graphs.BalancedTree(p,d) # a (p+1)-regular tree of depth
    d
G.delete_edge(G.edges()[0])
F = G.subgraph(G.connected_component_containing_vertex(0)) #
    A single 'flow'
H = N*F
H.add_cycle([len(F.vertices())*i for i in range(N)])
show(H)
#latex(H) # for the code
```

Theorem 3.1.17 Kohel. *Let V be an ordinary component of $G_l(\mathbf{F}_q)$ that doesn't contain 0 or 1728 then V is an l-volcano s.t.*

1. *All vertices in V_i have the same endomorphism ring O_i.*
2. *The subgraph on V_0 has degree*
$$1 + \left(\frac{\mathrm{disc}(K)}{l}\right)$$
where $K = \mathrm{Frac}(O_0)$
3. *If*
$$\left(\frac{\mathrm{disc}(K)}{l}\right) \geq 0$$
then $\#V_0$ is the order $[l]$ in $\mathrm{Cl}(O_0)$ else $\#V_0 = 1$.
4. *The depth of V is $d = v_l([O_K : \mathbf{Z}[\pi]])$ where π is the Frobenius morphism on any E with $j(E) \in V$.*
5. *$l \nmid [O_K : O_0]$, $[O_i : O_{i+1}] = l$ for $0 \leq i < d$.*

Application: Identifying supersingular elliptic curves.

Algorithm 3.1.18 Sutherland. *Input: Elliptic curve* E/k, char $k = p$. *Output: Ordinary or supersingular.*

1. *If* $j(E) \notin \mathbf{F}_{p^2}$ *then ordinary.*
2. *If* $p = 2, 3$ *return supersingular if* $j(E) = 0$ *or ordinary otherwise.*
3. *Find 3 roots of* $\phi_2(j(E), 4)$ *over* $\mathbf{F}_{p^2}$ *if not possible return ordinary.*
4. *Walk 3 paths in parallel for up to* $\lceil \log_2 p \rceil + 1$ *steps. If any of these paths get to* V_d, *return ordinary.*
5. *Otherwise supersingular.*

3.2 Supersingular isogeny graph cryptography (Asra)

Supersingular isogeny graph crypto is a candidate for post-quantum crypto, not based on factoring etc.

Recall last time we defined Ramanujan graphs, graphs with very good connectivity properties, a type of expander.

Proposition 3.2.1 *If* G *is a Ramanujan graph,* $x \in V$, $S \subseteq V$. *For a sufficiently large path beginning at* x, *the probability that the path ends in* S *is at least* $|S|/2|V|$.

Upshot: supersingular isogeny graphs are $(l + 1)$-regular, undirected, Ramanujan, connected (technically, Ramanujan means connected already, but its worth emphasising).

Some of our algorithms are only dependent on having a graph with this property, not so much the interpretation in terms of isogenies.

Supersingular isogeny graphs first appeared in crypto as potential hash functions.

3.2.1 Hash functions

(2010) (Charles, Goren, Lauter) proposed a cryptographically secure hash function based on the hardness of computing paths in a supersingular isogeny graphs.

Definition 3.2.2 Hash functions. A **hash function** is a deterministic function $h\colon \{0,1\}^* \to \{0,1\}^n$. ◊

Definition 3.2.3 Collision resistance. A hash function h is **collision resistant** if its hard to find x_1, x_2 with $x_1 \neq x_2$ s.t. $h(x_1) = h(x_2)$. ◊

Definition 3.2.4 Preimage resistance. A hash function h is **preimage resistant** if given $y \in \{0,1\}^n$ its hard to find x s.t. $h(x) = y$. ◊

Cool example, private set intersection, say two groups, Starbucks and BU want to find a list of common customers (students who bought something at Starbucks) but don't want to reveal anything to each other about the students or customers not in the intersection. Compute hashes of the names of customers and share the hashes, can compute the size of, and the intersection itself.

3.2.2 Supersingular isogeny hash functions

Parameters. $G_l(\mathbf{F}_{p^2})$, $p \equiv 1 \pmod{12}$, l to be small, fix an ordering on the edges, fix an initial vertex j_0 and an incoming edge.

Protocol. $m \in \{0,1\}^*$ write this as an l-bit string, $m \in \{0,1,\dots,l-1\}^*$, walk the graph based on m without backtracking.
Map the final j invariant to $\{0,1\}^{n \approx \log p}$.

Properties. Difficult means exponential in the size of the input normally.

Proposition 3.2.5

1. *Preimage resistant iff when given j it is difficult to compute a positive integer e and an isogeny $\phi\colon E_{j_0} \longrightarrow E_j$ with degree l^e.*

2. *Collision resistant iff when given j it is difficult to compute e and $\phi\colon E_{j_0} \longrightarrow E_{j_0}$ with degree l^e.*

3.2.3 Diffie-Hellman Key Exchange (1976)

Choose p, $\mathbf{Z}/p, g$ then Alice computes g^a send to Bob, he computes g^b and sends it back, they both compute g^{ab}, which is their shared secret.
The security is based on the hardness of computing g^{ab} given g^a, g^b.

3.2.4 Supersingular isogeny Diffie-Hellman (SIDH)

Parameters. Supersingular elliptic curve of smooth order: fix p to be big enough $p = l_A^{e_A} l_B^{e_B} f \pm 1$. l_A, l_B small primes, f is a number chosen such that p is big. Construct a supersingular elliptic curve E such that $\#E(\mathbf{F}_{p^2}) = (l_A^{e_A} l_B^{e_B} f)^2$, using Broker's algorithm.
Construct bases (P_A, Q_A) for $E[l_A^{e_A}]$, (P_B, Q_B) for $E[l_B^{e_B}]$.

Protocol. Alice takes $m_A, n_A \in \mathbf{Z}/l_A^{e_A}$
Bob takes $m_B, n_B \in \mathbf{Z}/l_B^{e_B}$
Alice finds $R_A = m_A P_A + n_A Q_A$
Bob finds $R_B = m_B P_B + n_B Q_B$
Alice finds $\phi_A\colon E \longrightarrow E/\langle R_A\rangle = E_A$
Bob finds $\phi_B\colon E \longrightarrow E/\langle R_B\rangle = E_B$
They send each other $E_i, \phi_i(P_i), \phi_i(Q_i)$.
Both compute $\phi'_A\colon E_B \longrightarrow E_B/\langle m_A\phi_B(P_A) + n_A\phi_B(Q_A)\rangle$ or analogous.
Shared secret is $j(E_{AB})$.

Hardness.

1. (Decisional supersingular isogeny problem) Given $E, (P_A, Q_A)$ a basis for $l_A^{e_A}$ torsion, let E_A be another curve, is E_A $l_A^{e_A}$ isogenous to E?

2. (Computational supersingular isogeny problem) Let $\phi_A\colon E \longrightarrow E_A$ be an isogeny with a kernel of the form $\langle m_A P_A + n_A Q_A\rangle$. Given E_A and $\phi_A(P_B)$ $\phi_A(Q_B)$, find R_A. $p^{1/4}$ classical, $p^{1/6}$ quantum.

3. Given $E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$ find j-invariant of E_{AB}.

3.2.5 Supersingular isogeny public key

Classically DH key-exchange $\rightsquigarrow$ ElGamal encryption.

1. Key generation.
   Alice: secret $\phi_A: E \to E_A$, public E_A and $\phi_A(P_B), \phi_A(Q_B)$.
2. Encryption.
   Bob: choose $\phi_B: E \to E_B$, compute $j(E_{AB})$.
   Send Alice $c = (E_B, \phi_B(P_A), \phi_B(Q_A), m \oplus j(E_{AB}))$
3. Decryption.
   Alice use $(E_B, \phi_B(P_A), \phi_B(Q_A))$ to compute $j(E_{AB})$. Computes $(m \oplus j(E_{AB})) \oplus j(E_{AB}) = m$.

$E(\mathbf{F}_{p^2})$, $p = l_A^{e_A} l_B^{e_B} f \pm 1$, for 128-bit security use a 512-bit key.

3.2.6 Algorithmic aspects

1. (Choosing f) Prime number theorem for arithmetic progressions gives you a bound on the density of primes of the form $l_A^{e_A} l_B^{e_B} f \pm 1$
2. Choosing a s.s. e.c. with the right group order, Broker's algorithm.
3. Finding a basis for $E[l_A^{e_A}]$.
   (a) Find a random point in $E(\mathbf{F}_{p^2})$ say P.
   (b) Check the order of $(l_B^{e_B} f)^2 \cdot P$. If its $l_A^{e_A}$ set $P_A = P$. Otherwise repeat from 1.
   (c) Do the same with $Q_A = Q$.
   (d) Check independence by seeing if $e(P_A, Q_A)$ has the right order, so that it is in $E[l_A^{e_A}]$ torsion.
4. Computing the kernels generated by $R_A = m_A P_A + n_A Q_A$, $m_A, n_A \in \mathbf{Z}/l_A^{e_A}\mathbf{Z}$. Analogue of double and add. Set $R_A = P_A + [m_A^{-1} n_A] Q_A$. Use differential addition (when you compute $A + B$ with side info $A - B$) and a Montgomery ladder
5. (Computing smooth degree isogenies) Decompose the $l_A^{e_A}$ isogeny into e_A different l_A-isogenies, $\phi_i: E_i \to E_{i+1}$ the kernel of ϕ_i is $\langle l_A^{e_A - i - 1} R_A \rangle$. Vélu's formula runs in $O(l)$ for l-isogeny.

3.3 Quaternion Algebras (Alex)

Q: Why study quaternion algebras?

A: They arise as the endomorphism algebras of *supersingular* elliptic curves $/\mathbf{F}_{p^2}$.

I don't want to spoiler next week at all, but I cannot talk about quaternion algebras without a little bit of motivation first!

Example 3.3.1 What are we doing again? Lets take

$$K = \mathbf{F}_9 = \mathbf{F}_3[\alpha] = \mathbf{F}_3[x]/(x^2 - x - 1)$$

and
$$E/K\colon y^2 = x^3 + \alpha x = f(x),$$
simple eh? It's supersingular as the j-invariant is 0 (and are in characteristic 3). Alternatively, count points or even compute the Hasse invariant, the coefficient of $p-1=2$ in $f(x)^{(p-1)/2=1}$, yep, it's 0.
We therefore have $\#E(K) = 9+1 = 10$ so we have a 2-torsion point ($P = (0,0)$) and any other point we can use to generate (will be 5 or 10 torsion). Let $x = 1$ so $y^2 = 1+\alpha = \alpha^2$ so $y = \pm\alpha$, say $Q = (1,\alpha)$.
We have one endomorphism, p-power frobenius $x \mapsto x^3$, $y \mapsto y^3$. How to find another one?
Lets compute an isogenous curve and see what happens! We will compute $\psi\colon E \longrightarrow E/\langle P\rangle = E'$. In general the formulae are a little annoying [71], when you have a 2-torsion point at $(0,0)$, not as bad:
$$\psi = \left(x + \frac{f'(0)}{x}, y - \frac{yf'(0)}{x^2}\right)$$
$$f'(0) = \alpha$$
so
$$\psi = \left(\frac{x^2+\alpha}{x}, y\frac{x^2-\alpha}{x^2}\right)$$
(aside: if $g/h = (x^2+\alpha)/x$ then $(g/h)' = (g'h - gh')/h^2 = (2x^2 - (x^2+\alpha))/x^2 = (x^2-\alpha)/x^2$, sanity check/fast computation?). The curve is then
$$E'\colon y^2 = x^3 + 0x^2 + (\alpha - 5\alpha)x + 0 = x^3 - \alpha x.$$
I think really here we're just recovering those classic formulae for 2-isogenies between curves with a rational 2 torsion point at $(0,0)$ (used in 2-descent).
$$\begin{aligned} C\colon y^2 &= x(x^2+ax+b)\\ D\colon v^2 &= u(u^2+a_1u+b_1)\\ \phi\colon C &\longrightarrow D\\ (x,y) &\mapsto ((y/x)^2, y - by/x^2)\\ \hat\phi\colon D &\longrightarrow C\\ (u,v) &\mapsto \left(\frac14\left(\frac{v}{u}\right)^2, \frac18(v - b_1v/u^2)\right)\end{aligned}$$
So far so good, our curve doesn't look exactly the same, but it's j-invariant is, so we are still in business. Is
$$E \simeq E'?$$
If we substitute $x = \alpha^2 x$, $y = \alpha^3 y$ into E' we get
$$\alpha^6 y^2 = \alpha^6 x^3 - \alpha^3 x$$
$$y^2 = x^3 - \alpha^{-3}x = x^3 + \alpha x,$$
call this map ι. Excellent, so to get $\psi'\colon E \longrightarrow E$ we compose $\iota\circ\psi$.
$$\iota\circ\left(\frac{x^2+\alpha}{x}, \frac{(x^2-\alpha)y}{x^2}\right) = \left(\alpha^2\frac{x^2+\alpha}{x}, \alpha^3\frac{(x^2-\alpha)y}{x^2}\right)$$
$$= \left((\alpha+1)\frac{x^2+\alpha}{x}, (-\alpha+1)\frac{(x^2-\alpha)y}{x^2}\right).$$

What happens to our other point Q? $\psi'(Q) = (\alpha^2(1+\alpha), \alpha^4(1-\alpha)) = (-1, \alpha-1)$

$$(0:0:1) \mapsto (0:1:0),\ (0:1:0) \mapsto (0:1:0),\ (1:\alpha:1) \mapsto (-1:\alpha-1:1),$$
$$(1:-\alpha:1) \mapsto (-1:-\alpha+1:1),\ (-1:\alpha-1:1) \mapsto (1:-\alpha:1),$$
$$(-1:-\alpha+1:1) \mapsto (1:\alpha:1),\ (\alpha:\alpha+1:1) \mapsto (-1:-\alpha+1:1),$$
$$(\alpha:-\alpha-1:1) \mapsto (-1:\alpha-1:1),\ (-\alpha:1:1) \mapsto (1:\alpha:1),\ (-\alpha:-1:1) \mapsto (1:-\alpha:1)$$

A word of caution: If you are very awake you may check and be led to believe that this is just the multiplication by -2 isogeny on E, its action on $E(\mathbf{F}_9)$ points is the same!!!!! It's not the same isogeny though so you can relax. Now we have an endomorphism ring with two elements, what are the relations between themselves, and each other?
As we quotiented by a rational 2-torsion point we have computed a factor of $\pi - 1$, the other factor comes from quotienting by 5-torsion. In fact we find. The frobenius has characteristic polynomial $t^2+9 = (t+3i)(t-3i)$ π looks like $3i$. ψ has characteristic polynomial $t^2-2t+2 = (t+1)^2+1$, so $\psi+1$ looks like $\pm i$. $?? \cdot \psi = \pi - 1$ $?? \cdot (i-1) = 3i-1$, so $?? = 2-i = 2-(\psi+1) = 1-\psi$.
So what if we quotient by non-rational 2-torsion? Pass to the quadratic extension $\mathbf{F}_{3^4}$, which we get from adjoining the other roots of $0 = x^3+\alpha x$ i.e. $\pm\sqrt{-\alpha}$. Denote this extension $\mathbf{F}_3[\beta]$, $(\beta^2-1)^2 = -\alpha$. We can use Vélu again, it's degree two still but a bit more ugh, you might need a computer from now on, actually I've been using one all along.

$$\phi = \left(\frac{(\alpha+1)\,x^2 + \left(-\beta^3-\beta-1\right)x}{x-(\beta^2-1)}, y\frac{(-\alpha+1)\,x^2 + \left(\beta^3-\beta^2+\beta-1\right)x - 1}{(x-(\beta^2-1))^2} \right)$$

doing a computation it looks like ϕ satisfies $\phi^2 - \phi + 2$.
What are the relations between these? Hopefully they generate the endomorphism ring by now but without relations we are screwed! Do they commute? Computing $\tau = \phi\psi - \psi\phi$ is relevant, if 0, commutative, otherwise not! Note that if they are algebraically dependant they must commute! In our example we can compute $\tau^2 + 3 = 0$ □

Finish this example, compute the endomorphism ring as a recognisable quaternion order.Aside: I now believe Asra when she says not to use Vélu's formulae for large degree!

Aside 2: Frobenius can be weird for supersingular curves, e.g. for

$$y^2 = x^3 + x/\mathbf{F}_9$$

we have $\pi = -3$. Or

$$y^2 = x^3 + 1/\mathbf{F}_{25}$$

we have $\pi = -5$

Indeed one can find on the internet claims like, all elliptic curves over finite fields have extra endomorphisms because frobenius exists!Show by hand that $y^2 + y = x^3/\mathbf{F}_4$ is supersingular and that frobenius is just the multiplication by -2 map.PODASIP: this happens for all p^2?

3.3.1 Quaternion Algebras

Pretty much all of this material was ripped with the utmost love and affection from [72], check it out.

Proposition 3.3.2 *The theory of Quaternion algebras is very rich.*

Proof. The above book is 800 pages long. ■

So now we have gone out into nature and observed a beautiful new species of algebra, time to catch it, pin it to a wall, dissect it to study it in detail. It might not look as pretty any more but it's the way the science is done.

Example 3.3.3 Hamilton's quaternions. Hamilton's quaternions $\mathbf{H}$ were the first quaternion algebra to be discovered (citation needed). The structure is like two copies of $\mathbf{C}$ tensored together in some non-commuting way over $\mathbf{R}$. We have a real algebra with two generators i, j s.t. $i^2 = j^2 = (ij)^2 = -1$ we let $k = ij$ for aesthetic reasons (note that these relations imply noncommutativity!). Like this we get a division algebra. □

Quaternion algebras are a generalisation of this to other fields.

Definition 3.3.4 Quaternion algebras. Let F be a field (not characteristic 2), a quaternion algebra over F is an algebra B over F for which there exist $a, b \in F^\times$ such that there is a basis

$$1, i, j, k \in B$$

such that

$$i^2 = a, j^2 = b, k = ij = -ji,$$

it is automatic that $k^2 = -ab$ from this.
We denote this particular quaternion algebra by $\left(\frac{a,b}{F}\right)$ ◊

Example 3.3.5

$$\mathbf{H} = \left(\frac{-1,-1}{\mathbf{R}}\right).$$

□

Example 3.3.6 What is

$$\left(\frac{1,1}{F}\right)\left(= \left(\frac{1,-1}{F}\right)\right)?$$

We have another way to come up with 4-dimensional non-commutative algebras over fields, matrices! Let

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

so

$$k = ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -ji$$

as required. □

Call this example *split*, in analogy with quadratic theory, If $x^2 - N$ has a solution mod p then $\left(\frac{N}{p}\right) = 1 = \left(\frac{1}{p}\right)$.

Note that if a or $b \in (F^\times)^2$ then we can divide the corresponding basis element by $\sqrt{a}$ or whatever and find that $\left(\frac{a,b}{F}\right) = \left(\frac{1,b}{F}\right)$. This shows:

Proposition 3.3.7 *After passing to the algebraic closure (or even the quadratic closure!) every quaternion algebra is split.*

This is helpful as it allows us to work with non-split quaternion algebras as matrix algebras over a quadratic extension.

Example 3.3.8 $\mathbf{H}/\mathbf{R}$ can be seen as $\mathrm{Mat}_{2\times 2}(\mathbf{R}(i)) = \mathrm{Mat}_{2\times 2}(\mathbf{C})$, explicitly

$$i = i\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$$

$$j = i\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

please excuse the unfortunate notational clash here, I hope you agree it's somewhat unavoidable. □

Here is a nice lemma I probably used implicitly already somewhere!

Lemma 3.3.9 *An F-algebra B with F-algebra generators i, j satisfying $i^2, j^2 \in F^\times$, $ij = -ji$ is automatically a quaternion algebra (i.e. dimension 4).*

Proof. Show linear independence of $1, i, j, ij$ (exercise). ■

Definition 3.3.10 Conjugate, trace and norm. Given a quaternion algebra B/F there is a unique anti-involution $\bar{\cdot}\colon B \to B$, called **conjugation**.
With basis $1, i, j, ij \in \left(\frac{a,b}{F}\right)$ as above it is given as

$$\overline{x + yi + zj + wij} = x - yi - zj - wij,\ x, y, z, w \in F.$$

As normal (heh) we define the (reduced) norm and trace

$$\mathrm{Norm}\,\alpha = \alpha + \overline{\alpha},\ \forall \alpha \in B$$

$$\mathrm{Norm}(x + yi + zj + wij) = x^2 - ay^2 - bz^2 + abw^2$$

and

$$\mathrm{Tr}\,\alpha = \alpha + \overline{\alpha},\ \forall \alpha \in B$$

$$\mathrm{Tr}(x + yi + zj + wij) = 2x.$$

◊

3.3.1.1 Orders

In our example, while the endomorphism algebra $\mathrm{End}(E) \otimes \mathbf{Q}$ was of interest, the endomorphism ring $\mathrm{End}(E)$ was the more fundamental object. What is this? A quaternion ring?

Definition 3.3.11 Orders in quaternion algebras. Let $B/\mathbf{Q}$ be a quaternion algebra, an **order** in B is a full rank sub-$\mathbf{Z}$-module that is also a subring. ◊

Example 3.3.12 The Lipschitz order. $B = \left(\frac{-1,-1}{\mathbf{Q}}\right)$ (Hamilton quaternions with $\mathbf{Q}$-coefficients) then we have an order

$$\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}ij$$

the **Lipschitz order**. □

Definition 3.3.13 Maximality. Orders are ordered (heh) with respect to inclusion, thus we get notions of maximality of orders etc. ◊

Is the Lipschitz order maximal? NO! Whats going on? $\mathbf{Z}[i]$ is maximal in $\mathbf{Q}(i)$ after all. Consider

$$i + j + k,\ (i + j + k)^2 = i^2 + j^2 + k^2 + \cancelto{0}{ij + ji} + \cancelto{0}{ik + ki} + \cancelto{0}{jk + kj} = -3$$

so we have a $\mathbf{Z}[\sqrt{-3}]$ lurking inside $\left(\frac{-1,-1}{\mathbf{Q}}\right)$, quaternion algebras are not everything they appear to be at first sight! $\mathbf{Z}[\sqrt{-3}]$ is non-maximal and we must add $\sqrt{-3}/2$ to make it so. Lets add this in the quaternion setting:

Example 3.3.14 The Hurwitz order. Let $B = \left(\frac{-1,-1}{\mathbf{Q}}\right)$, then

$$\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}\left(\frac{i + j + k}{2}\right)$$

is an index two suborder of the Lipschitz order, called the **Hurwitz order**, this *is* maximal. □

Warning, just because $\sqrt{-3} \in \left(\frac{-1,-1}{\mathbf{Q}}\right)$ we do not have $\left(\frac{-1,-3}{\mathbf{Q}}\right) = \left(\frac{-1,-1}{\mathbf{Q}}\right)$!

Example 3.3.15 /Exercise. Show that the elliptic curve from the exercise earlier

$$y^2 + y = x^3/\overline{\mathbf{F}_2}$$

has endomorphism algebra the Hurwitz order.

Solution. Here is what me and Angus think, we have the 2-power frobenius π a degree 2 isogeny whose square is minus 2, we also have the isogeny $\phi\colon x \mapsto \zeta_3 x, y \mapsto y$ which is in fact an automorphism (degree 1) and satisifies $\phi^2+\phi+1 = 0$. The relation between these two isogenies is that $\pi\phi = \phi^2\pi\colon x \mapsto \zeta_3^2 x^2, y \mapsto y^2$.
Inside the Huwitz order we have some candidates for an element whose square is -2 there are a few, coming in two types $a + b$ for $a \neq b \in \{i, j, k\}$ and $a - b$ for $a \neq b \in \{i, j, k\}$, we choose the second type (why? because it works and the other doesn't), let $p = i + j$ for concreteness. We also have a cube root of unity in the Hurwitz order, it is $f = (-1 + i + j + k)/2$.
We can calculate now what pf and f^2p are, they both come out to be $-i + k$, some other square root of minus 2, which makes sense because degree is multiplicative. Anyway this is consistent with the endomorphism ring but there is a slight problem, the order generated here has discriminant 6, so its non-maximal as we know its contained in the Hurwitz order but the discriminant is higher, Deuring tells us we have to get a maximal order so we need something extra. □

Warning, there is no such thing as *the* maximal order of a quaternion algebra! Rather there are multiple maximal orders due to non-commutativity, e.g. if $\mathcal{O}$ is a maximal order then so is

$$\alpha\mathcal{O}\alpha^{-1} \neq \mathcal{O}.$$

Normally when we have unique maximal things with a certain property, its because we can always take spans/unions and they still have that property.

This is no longer true here, the sum of two elements with integral trace and norm need not remain so, nor the product.

We can define discriminants of orders which like normal give a hint as to their maximality

$$\mathcal{O} = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}ij \subseteq \left(\frac{a, b}{\mathbf{Q}}\right)$$

$$\operatorname{disc} O = d(1, i, j, ij) = \left|\det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2a & 0 & 0 \\ 0 & 0 & 2b & 0 \\ 0 & 0 & 0 & -2ab \end{pmatrix}\right| = (4ab)^2$$

Exercise 3.3.16 Find the discriminant of the Lipschitz order.

3.3.1.2 Local theory

Theorem 3.3.17 *Over a local field $F \neq \mathbf{C}$ there is a unique division quaternion algebra B/F up to F-isomorphism.*
If $F = \mathbf{Q}_p$, $p \neq 2$ then this is

$$\left(\frac{e, p}{\mathbf{Q}_p}\right)$$

for e any quadratic non-residue mod p.
This is saying that any quadratic extension of F embeds into B!

Definition 3.3.18 Split and ramified quaternion algebras. Let $B/\mathbf{Q}_v$ be a quaternion algebra, we say that B is

$$\begin{cases} \text{split} & \text{if } B \cong M_2(\mathbf{Q}_v) = \left(\frac{1,-1}{\mathbf{Q}_v}\right) \\ \text{ramified} & \text{otherwise} \end{cases}$$

Correspondingly we say that $B/\mathbf{Q}$ is split/ramified at a place v if the corresponding $B \otimes \mathbf{Q}_v$ has that property. ◊

The terminology definite for quaternion algebras ramified at infinity is also used (i.e. for which $B \otimes \mathbf{R} = \mathbf{H}$).

Theorem 3.3.19 Albert-Brauer-Hasse-Noether. *Let B/F be a quaternion algebra over a number field F (or any central simple algebra), if B splits at every place v of F then B is a matrix algebra $M_d(F)$.*

In fact:

Theorem 3.3.20 *Two quaternion algebras are isomorphic if and only if they are isomorphic everywhere locally, i.e. if the set of places at which they ramify is the same.*

Warning: Quaternion algebras may not be ramified where you think they are?

Knowing the ramification of a quaternion algebra $\mathbf{Q}$ is enough to identify it uniquely, in fact we have the following theorem

Theorem 3.3.21 Main Theorem [72, 14.1.3]. *There is a sequence of bijections*

$$\begin{gathered} \{\textit{quaternion algebras } B/\mathbf{Q}\}\ /\textit{isom.} \\ S \mapsto \textit{unique } B \textit{ ramified at exactly } S \updownarrow D \mapsto \{p : B \textit{ is ramifies at } p\} \\ \{S \subseteq \textit{places of } \mathbf{Q},\ 2|\#S\} \\ D \mapsto \{p|D\} \cup \{\infty\} \textit{ if } 2 \nmid \omega(D) \updownarrow S \mapsto \prod_{p \in S, p \neq \infty} p \\ \{D \in \mathbf{Z}_{>0} \textit{ squarefree}\} \end{gathered}$$

Sometimes however we want generators and relations not just ramification information: (As we will only care about discriminant p quaternion algebras) In our setting the relevant theorem is:

Theorem 3.3.22 Pizer. *Let $\mathbf{Q}_{p,\infty}$ be the unique quaternion algebra ramified at p, ∞, let $q \equiv 3 \pmod 4$ be such that $\left(\frac{p}{q}\right) = -1$, then*

$$\mathbf{Q}_{p,\infty} \cong \begin{cases} \left(\frac{-1,-1}{\mathbf{Q}}\right) & \text{if } p \equiv 2 \pmod 4, \\ \left(\frac{-1,-p}{\mathbf{Q}}\right) & \text{if } p \equiv 3 \pmod 4, \\ \left(\frac{-2,-p}{\mathbf{Q}}\right) & \text{if } p \equiv 1 \pmod 8, \\ \left(\frac{-p,-q}{\mathbf{Q}}\right) & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Ibukiyama has given a nice description of a maximal order in such.
Here are some nice references:

1. Computational Problems in Supersingular Elliptic Curve Isogenies - Steven D. Galbraith and Frederik Vercauteren https://www.esat.kuleuven.be/cosic/publications/article-2842.pdf
2. Computing Isogenies Between Abelian Varieties - David Lubicz Damien Robert https://perso.univ-rennes1.fr/david.lubicz/articles/isogenies.pdf
3. Toric forms of elliptic curves and their arithmetic - Wouter Castryck and Frederik Vercauteren https://homes.esat.kuleuven.be/~fvercaut/papers/ec_forms.pdf
4. Isogenies of Elliptic Curves: A Computational Approach - Daniel Shumow https://www.sagemath.org/files/thesis/shumow-thesis-2009.pdf
5. Hard and Easy Problems for Supersingular Isogeny Graphs - Christophe Petit and Kristin Lauter https://eprint.iacr.org/2017/962.pdf
6. Perspectives on the Albert-Brauer-Hasse-Noether Theorem for Quaternion Algebras - Thomas R. Shemanske https://www.math.dartmouth.edu/~trs/expository-papers/tex/ABHN.pdf
7. COMPUTING ISOGENIES BETWEEN SUPERSINGULAR ELLIPTIC CURVES OVER Fp CHRISTINA DELFS AND STEVEN D. GALBRAITH http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.740.6509&rep=rep1&type=pdf

3.4 The Deuring Correspondence (Maria Ines)

References:

1. Voight ch. 16,17,42
2. Hard and Easy Problems for Supersingular Isogeny Graphs - Christophe Petit and Kristin Lauter https://eprint.iacr.org/2017/962.pdf

3.4.1 Background: Ideals and Ideal classes

Let $B/\mathbf{Q}$ be a quaternion algebra and $O \subseteq B$ be an order. If $I \subseteq B$ is a lattice, we can define $O_L(I) = \{\alpha \in B : \alpha I \subseteq I\}$. This is an order , it's the left order of I similarly can define $O_R(I)$.

Definition 3.4.1 A left (resp. right) fractional ideal is a lattice $I \subseteq B$ s.t. $\mathcal{O} \subseteq \mathcal{O}_L(I)$ resp $\mathcal{O} \subseteq \mathcal{O}_R(I)$ ◊

Definition 3.4.2 Compatibility. For lattices $I, J \subseteq B$ we say I is **compatible** with J if

$$\mathcal{O}_R(I) = \mathcal{O}_L(J).$$

A lattice I is invertible if there is a lattice $I' \subseteq B$ s.t.

$$II' = \mathcal{O}_L(I) = \mathcal{O}_R(I')$$

$$I'I = \mathcal{O}_L(I') = \mathcal{O}_R(I)$$

with both products compatible ◊

Proposition 3.4.3 *Let $\mathcal{O} \subseteq B$ be a maximal order then every left or right fractional $\mathcal{O}$-ideal is invertible.*

Definition 3.4.4 Principal ideals. An ideal of the form

$$I = \mathcal{O}_L(I)\alpha = \alpha\mathcal{O}_R(I)$$

is a principal ideal. ◊

Fact 3.4.5 *I is invertible with $I^{-1} = \alpha^{-1}\mathcal{O}_L(I) = \mathcal{O}_R(I)\alpha^{-1}$.*

Definition 3.4.6 Reduced norms. Let $I \subseteq B$ be a fractional ideal the **reduced norm** of I is the positive generator of the fractional ideal generated by

$$\{\operatorname{nrd}(\alpha) : \alpha \in I\}$$

in $\mathbf{Q}$. We denote it $\operatorname{nrd}(I)$. ◊

Ideal classes.

Definition 3.4.7 Ideal classes. Two left fractional ideals $I, J \subseteq B$ are in the same left class

$$I \sim_L J$$

if $\exists \alpha \in B^\times$ s.t. $I\alpha = J$. Equivalently if $\mathcal{O}_L(I) = \mathcal{O}_L(J)$ and $I \sim J$ as left modules over this order. $\sim_L$ is an equivalence relation $[I]$ is the class of I. If I is invertible then every $J \in [I]_L$ is invertible, and then we say $[I]_L$ is invertible. ◊

Definition 3.4.8 Class sets. Let $\mathcal{O} \subseteq B$ be an order. The **left class set** of $\mathcal{O}$ is

$$\operatorname{Cls}_L \mathcal{O} = \{[I]_L : I \subseteq B \text{ is invertible and } \mathcal{O}_L(I) = \mathcal{O}\}$$

its a pointed set with distinguished element $[\mathcal{O}]_L$. ◊

Theorem 3.4.9 *Let $\mathcal{O} \subseteq B$ be an order. then $\operatorname{Cls}_L \mathcal{O}$ is finite. We call $\#\operatorname{Cls}_L \mathcal{O}$ the **left class number** of $\mathcal{O}$.*

Types of orders. Let $\mathcal{O}, \mathcal{O}' \subseteq B$ be orders.

Definition 3.4.10 We say $\mathcal{O}, \mathcal{O}'$ are of the same type if $\exists \alpha \in B^\times$ s.t. $\mathcal{O}' = \alpha^{-1}\mathcal{O}\alpha$. $\mathcal{O}, \mathcal{O}'$ are locally of the same type if $\mathcal{O}_p, \mathcal{O}'_p$ are of the same type for all primes in $\mathbf{Z} \cup \{\infty\}$. $\mathcal{O}$ is connected to $\mathcal{O}'$ if there exists an invertible fractional $\mathcal{O}, \mathcal{O}'$-ideal $J \subseteq B$ called a connecting ideal. ◊

Lemma 3.4.11 *$\mathcal{O}, \mathcal{O}'$ are of the same type iff they are isomorphic as $\mathbf{Z}$-algebras. $\mathcal{O}, \mathcal{O}'$ are connected iff they are locally of the same type.*

Definition 3.4.12 Let $\mathcal{O} \subseteq B$ be an order.

1. The **genus** $\mathrm{Gen}(\mathcal{O})$ of $\mathcal{O}$ is the set of orders in B connected to $\mathcal{O}$.
2. The type set $\mathrm{Typ}(\mathcal{O})$ of $\mathcal{O}$ is the set of $\mathbf{Z}$-algebra isomorphism classes of orders in $\mathrm{Gen}(\mathcal{O})$.

$\lozenge$

Lemma 3.4.13 *The set map* $\mathrm{Cls}_L(\mathcal{O}) \to \mathrm{Typ}(\mathcal{O})$

$$[I]_L \mapsto \text{class of } \mathcal{O}_R(I)$$

is surjective.

Remark 3.4.14

1. Any two maximal orders in B are connected.
2. In particular there are only finitely many conjugacy classes of maximal orders in B.

Example 3.4.15 Voight 17.6.3. Let

$$B = \left(\frac{-1, -23}{\mathbf{Q}}\right)$$

Then $\mathcal{O} = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}\frac{i+j}{2} + \mathbf{Z}i\frac{i+j}{2}$ is a maximal order and

$$\mathrm{Typ}(\mathcal{O}) = \{[\mathcal{O}], [\mathcal{O}_2], [\mathcal{O}_3]\}.$$

$\square$

3.4.2 The Deuring Correspondence

Fix a prime p, let E be an elliptic curve over $\mathbf{F}_q = \mathbf{F}_{p^n}$.

Lemma 3.4.16 *The endomorphism algebra $\mathrm{End}(E)_{\mathbf{Q}} = \mathrm{End}(E) \otimes \mathbf{Q}$ of E is either $\mathbf{Q}$ an imaginary quadratic field or a definite quaternion algebra $/\mathbf{Q}$.*

Theorem 3.4.17 Deuring, this proof by Lenstra. *Let $E/\mathbf{F}_q$ be a s.s. e.c. (i.e. assume $\mathrm{End}(E) \otimes \mathbf{Q}$ is a quaternion algebra). Then $\mathrm{Ram}(B) = \{p, \infty\}$ and $\mathcal{O} = \mathrm{End}(E)$ is a maximal order in B.*

Proof. Let $n > 0$ be prime to p. Then

$$E[n] \simeq \mathbf{Z}/n \oplus \mathbf{Z}/n$$

as groups so $\mathrm{End}(E[n]) \simeq M_2(\mathbf{Z}/n)$.

Claim: The structure map $\mathcal{O}/n\mathcal{O} \to \mathrm{End}(E[n])$ is an isomorphism.

Check: suppose $\phi \in \mathcal{O}$ kills $E[n]$, then since ϕ is separable then $\exists\, \psi \in \mathcal{O}$ s.t. $\phi = n\psi$. Hence $\phi = 0 \in \mathcal{O}/n$. This gives injectivity.

As both rings are finite with the same order n^4 we have an isomorphism.

Since $\mathcal{O}$ is a free $\mathbf{Z}$ module

$$\mathcal{O}_l = \mathcal{O} \otimes \mathbf{Q}_l = \mathcal{O} \otimes \varprojlim_n \mathbf{Z}/l^n$$

$$\simeq \varprojlim_n \mathcal{O}/l^n \simeq \varprojlim_n \operatorname{End}(E[l^n])$$

$$\simeq \operatorname{End}_{\mathbf{Z}_l} \simeq M_2(\mathbf{Z}_l)$$

for any $l \neq p$ primes. This is an isomorphism as $\mathbf{Z}$-algebras.

In particular $\mathcal{O}_l$ is maximal in $B_l \simeq M_2(\mathbf{Q}_l)$ and B is split at l for all $l \neq p$. Since B is definite, it follows from the classification theorem that $\operatorname{Ram}(B) = \{p, \infty\}$.

Fact: $\mathcal{O}_p$ is maximal in B_p (thm 42.1.9 of voight).

$\mathcal{O}$ is maximal in B because it is locally maximal. ■

Theorem 3.4.18 Deuring correspondence.

$$\left\{\textit{maximal orders } \mathcal{O} \subseteq B_{p,\infty}\right\}/\sim \leftrightarrow \left\{j \textit{ s.s. } \in \mathbf{F}_{p^2}\right\}/\operatorname{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p).$$

Proof. Voight 42.4.7. ■

Definition 3.4.19 Let $I \subseteq \mathcal{O} = \operatorname{End}(E)$ be an integral left $\mathcal{O}$-ideal with $(\operatorname{nrd}(I), p) = 1$. Define

$$E[I] = \{P \in E(\overline{\mathbf{F}}_q) : \alpha(P) = 0 \forall \alpha \in I\}$$

Then there is a separable isogeny

$$\Phi_I : E \longrightarrow E/E[I]$$

with $\ker \Phi_I = E[I]$. ◊

Fact 3.4.20

$$\deg(\Phi_I) = \operatorname{nrd}(I)$$

Proposition 3.4.21 *The association $I \mapsto \phi_I$ is a 1-1 correspondence provided that* $(\deg \phi_I, p) = 1$.

3.4.3 Applications to SIG crypto

Problem 3.4.22 Constructive Deuring correspondence. Given a maximal order $\mathcal{O} \subseteq B_{p,\infty}$ return a s.s. j-invariant j s.t. $\mathcal{O} \simeq \operatorname{End}(E_j)$. □

Problem 3.4.23 Inverse Deuring correspondence. Given a supersingular j invariant j, compute a maximal order $\mathcal{O} \subseteq B_{p,\infty}$ s.t. $\mathcal{O} \simeq \operatorname{End}(E_j)$. $\mathcal{O}$ is described by a $\mathbf{Z}$-basis. □

Problem 3.4.24 Endomorphism ring computation problem. Given a supersingular j invariant j, $\operatorname{End}(E_j)$. $\operatorname{End}(E_j)$ should be returned as 4 or 3 rational maps that form a $\mathbf{Z}$-basis. Their representation should be efficient in storage and in evaluation time at points. □

Remark 3.4.25

1. Problem 1 can be solved in polynomial time, (Prop. 14 in Petit-Lauter).
2. P2 and P3 are polynomially equivalent but this isn't obvious (P-L sec.3.1 and 3.2)
3. There is no known efficient algorithm to solve P3.

Recall: the (Charles-Goren-Lauter) CGL hash function is preimage resistant iff given 2 s.s. j-invariants j_1, j_2 its computationally hard to compute a positive integer e and an isogeny $\phi\colon E_{j_1} \longrightarrow E_{j_2}$ of degree l^e.

Proposition 3.4.26 *Assume there's an efficient algorithm to solve P3. Then there is an efficient algorithm to solve the preimage problem for the CGL hash function*

Proof. Algorithm
Input: two s.s. j-invariants $j_s, j_t \in \mathbf{F}_{p^2}$.
Output: sequence of j-invariants

$$j_s, \dots, j_0, \dots, j_t.$$

1. Compute $\mathrm{End}(j_s), \mathrm{End}(j_t)$.
2. Compute $\mathcal{O}_s \simeq \mathrm{End}(E_{j_s}), \mathcal{O}_t \simeq \mathrm{End}(E_{j_t})$
3. Compute ideals I_s and I_t connecting $\mathcal{O}_0$ to $\mathcal{O}_s, \mathcal{O}_t$
4. Compute ideals $J_s \in [I_s], J_t \in [I_t]$, with norms l^{e_s}, l^{e_t}.
5. For $J \in \{J_s, J_t\}$ and corresponding $E \in \{E_s, E_t\}$ and $e \in \{e_s, e_t\}$ compute $J_i = \mathcal{O}_0 p^2 + \mathcal{O}_0 l^i$ for $i = 0, \dots, e$. For $i = 0, \dots, e$ compute $K_i \in [J_i]_L$ with powersmooth norm. Translate K_i into an isogeny

$$\phi\colon E_0 \longrightarrow E_i$$

   Deduce a sequence $(j_0, j(E_1), \dots, j(E) = j_e)$.
6. Return $(j(E_s), \dots, j_0, \dots, j(E_t))$.

Except for step 1 everything can be done efficiently. ∎

Remark 3.4.27 The converse is also true.

Chapter 4

p-divisible groups

These are notes for the short-lived BUNTES Fall 2018 part II, the topic is p-divisible groups.

http://math.bu.edu/people/midff/buntes/fall2018.html.

References:

1. Tate
2. Schatz

4.1 p-divisible groups (Sachi)

Why study p-divisible groups (Jacob Stix).

1. Analyse local p-adic galois action on p-torsion of elliptic curves, Serre's open image theorem.
$$\phi_l : G_K \to \mathrm{Aut}[l]$$
Surjective for almost all l.
2. Tool for representing p-adic cohomology, e.g p-adic hodge theory.
3. Describe local properties of moduli spaces of abelian varieties which map to moduli spaces of p-divisible groups which can be described by semilinear algebra (Serre-Tate).
4. Explicit local CFT via Lubin-Tate formal groups describing wildly ramified abelian extensions.
5. The true fundamental group in characteristic p must include infinitesimal group schemes, p-divisible groups enter through their tate modules.

Detour, schemes. There is an (anti)-equivalence of categories
$$\{\text{ring}\} \leftrightarrow \{\text{affine schemes}\}.$$

Moral whatever a scheme is the data of a ring is enough to specify it + homs
$$\mathrm{Hom}_{Ring}(B, A) \leftrightarrow \mathrm{Hom}_{Aff}(\mathrm{Spec}\, A, \mathrm{Spec}\, B)$$

to specify a base field or base ring play a similar game with R-algebras and R-schemes.

Yoneda, schemes are functors: Let $R[T_1, \dots, T_n]$ be a polynomial ring over R, we want solutions to

$$f_1 = f_2 = \cdots = f_m = 0$$

with coefficients in A this is asking for a map

$$R[T_1, \dots, T_n]/(f_i) \to A$$

same as

$$\mathrm{Hom}_{R-alg}(R[T_1, \dots, T_n]/(f_i), A)$$

functor A to this is a functor from R-algs to sets.

Definition 4.1.1 For any affine scheme $A = \operatorname{Spec} B$ we attach a functor h_X from $\mathrm{Sch}^{\mathrm{op}}$ to sets, sending $\operatorname{Spec} S \mapsto \mathrm{Hom}_{\mathrm{Sch}}(\operatorname{Spec} S, X) = \mathrm{Hom}_{Ring}(B, S) = h_X(\operatorname{Spec} S)$. spec S points of X ◊

Example 4.1.2

$$\mathbf{A}^n = \operatorname{Spec} \mathbf{Z}[T_1, \dots, T_n]$$

$$\mathbf{A}^n(T) = \mathrm{Hom}_{\mathrm{Sch}}(T, \mathbf{A}^n) = \mathrm{Hom}_{Ring}(\mathbf{Z}[T_1, \dots, T_n], S) \cong S^n$$

□

Example 4.1.3

$$E\colon \operatorname{Spec} k[x, y]/(y^2 - (x^3 + ax + b)),\ k = \mathbf{Q}$$

$E(\mathbf{Q}(i)) = \mathbf{Q}(i)$ points, choosing x, y satisfying weierstrass equation. □

Suppose $h_X\colon \mathrm{Sch}^{\mathrm{op}} \to R$ factors through Grp $\to$ Set then this is a group scheme.

Example 4.1.4

$$\mathbf{G}_a = \operatorname{Spec} k[t]$$

$$S \mapsto \mathrm{Hom}(k[t], S) \cong (S, +)$$

□

Example 4.1.5

$$\mathbf{G}_m = \operatorname{Spec} k[t, t^{-1}]$$

$$S \mapsto \mathrm{Hom}(k[t, t^{-1}], S) \cong (S^\times, \cdot)$$

□

Example 4.1.6

$$\mu_n = \operatorname{Spec} k[t]/(t^n - 1)$$

□

Example 4.1.7

$$\alpha_{p^n} = \operatorname{Spec} k[t]/(t^{p^n})$$

char $k = p$ □

Cartier Duality G is a finite group scheme $/R$ there is a dual

$$G^*(T) = \mathrm{Hom}(G_T, \mathbf{G}_m)$$

R-scheme T

$$G \cong (G^*)^*$$

Example 4.1.8

$$\mu_{p^n} \leftrightarrow \mathbf{Z}/p^n$$

□

Definition 4.1.9 Let p be a prime and h a non-negative integer. A p-divisible group of height h is an inductive system

$$(G_v, i_v)$$

where each G_v is a group scheme $/R$ of size p^{vh}

$$i_v : G_v \to G_{v+1}$$

identifies G_v with kernel of multiplication by p^v.

$$0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{[p^v]} G_{v+1}$$

◊

Remark 4.1.10 We can show that G_μ, G_v are two levels then

$$0 \to G_\mu \xrightarrow{i_{\mu,v}} G_{\mu+v} \xrightarrow{[p^\mu]} G_{\mu,v}$$

so

$$0 \to G_\mu \to G_{\mu+v} \to G_v \to 0.$$

The connected etale sequence

A finite flat group scheme G over a henselian local ring R admitsa (functorial) decomposition

$$0 \to G^\circ \to G \to G^{\mathrm{et}} \to 0$$

connected and etale

There is an equivalence of categories between finite etale gp scheme $/R$ and its continuous $\mathrm{Gal}(\overline{k}/k)$ modules when $R = k$ is a field.

Definition 4.1.11 An n-dimensional formal lie group $/R$ is the formal power series ring

$$A = R[[x_1, \ldots, x_n]]$$

with a suitable co-multiplication structure.

$$m^* : A \to A \widehat{\otimes} A$$

$$m^*(X_i) = (f_i(Y, Z))$$

require

1. $$F(X, 0) = F(0, X) = X$$

2. $$F(X, F(Y, Z)) = F(F(Y, Z), X) = X$$

3. $$F(Y, Z) = F(Z, Y)$$

◊

Let ψ denote multiplication by p in A then A is divisible if ψ is an isogeny (surj. with finite kernel). Alternatively A is a finite free $\psi(A)$-module.

Theorem 4.1.12 *Let R be a complete noetherian local ring with residue characteristic $p > 0$. We have an equiv of cats*

$$\textit{conn. p-div gps} \leftrightarrow \textit{div. formal lie groups } /R$$

Example 4.1.13

$$\mathbf{G}_m(p),\ F(X) = Y + Z + YZ$$

□

Example 4.1.14 E ordinary elliptic curve $/\overline{\mathbf{F}}_p$

$$E[p](\overline{\mathbf{F}}_p)$$

is non-empty

$$E[p] = E[p]^\circ \times E[p]^{\mathrm{et}}.$$

etale group schemes over alg. closed fields are constant

$$E = E[p]^\circ \times A$$

It can't be entirely etale $[p]$ would be etale but this induces the 0 map on tangent space so $E[p]^\circ \neq 0$.

$$|E[p]| = p^2$$

so each order p.

$$A = \mathbf{Z}/p$$

E is cartier self dual

$$A^* = \mu_p = E[p]^\circ$$

Induct for $E[p^n]$. □

Chapter 5

Shimura varieties

These are notes for BUNTES Fall 2018 part III, the topic is Shimura varieties http://math.bu.edu/people/midff/buntes/fall2018.html.

Outline:

1.

References:

5.1 Modular curves (Aash)

Definition 5.1.1 Lattices. A **lattice** is a free abelian group of rank 2

$$\Lambda \otimes \mathbf{R} \to \mathbf{C}$$

is an isomorphism

$$\Lambda = \mathbf{Z}[\alpha] \oplus \mathbf{Z}[\beta]$$

if

$$\Lambda = \gamma\Lambda',\ \gamma \in \mathbf{C}$$

then we say the two lattices are **homothetic**. ◊

Any lattice is homothetic to one of the form

$$\Lambda = \langle 1, \tau \rangle$$

as we can take a positively oriented basis we have that all such are equivalent to

$$\tau \in \mathbf{H} = \{z \in \mathbf{C} : \Im(z) > 0\}.$$

So there is a bijection between $\mathbf{H}$ and ordered bases of lattices.

$\mathrm{SL}_2(\mathbf{Z})$ acts on $\mathbf{H}$ and the action corresponds to changing bases.

The action of $\mathrm{PSL}_2(\mathbf{Z})$ is faithful. $i, \rho = e^{\pi i/3}$ have non-trivial stabilisers

$$\mathrm{Stab}_i = \langle S \rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\mathrm{Stab}_\rho = \langle TS \rangle,\ T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

We can determine the order of elements by looking at the characteristic polynomials.

We then have

$$Y(1) = \mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$$

a complex manifold and

$$j\colon Y(1) \to \mathbf{C}$$

is an isomorphism.

We have a fundamental domain for this action

$$D = \{z \in \mathbf{C} : |z| \geq 1, |\Re(z)| \leq \frac{1}{2}\}$$

$Y(1)$ is Hausdorff because the action is properly discontinuous.

Care must be taken around the elliptic points (those with larger stabiliser), to define the complex structure.

The extended upper half plane

$$\mathbf{H}^* = \mathbf{H} \cup \mathbf{P}^1(\mathbf{Q})$$

also has an $\mathrm{SL}_2(\mathbf{Z})$ action via fractional linear transformations, which is proper.

We can define a basis of neighbourhoods around the cusps by transforming them to the cusp ∞ where we can use the basis of neighbourhoods given by

$$\mathbf{H}_N = \{z \in \mathbf{H} : |\Im(z)| > N\}.$$

The parameter q around ∞ is defined as $e^{2\pi i z/N}$ for some $N \in \mathbf{Z}$, q is fixed by T.

We can quotient by the action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{H}^*$ to get

$$X(1) = \mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}^*$$

which is now compact, genus 0, which matches up with $Y(1)$ having $\mathbf{C}$ points $\mathbf{C}$ earlier.

If X is a projective curve then $X(\mathbf{C})$ has the structure of a compact Riemann surface. If S is such a surface then there exists a unique up to isomorphism X with $X(\mathbf{C}) = S$.

The meromorphic functions on S are the function field of X and there is a correspondence

$$\text{Compact Riemann surfaces} \leftrightarrow \text{Smooth proj. curves}$$

Given a finite index subgroup of $\mathrm{SL}_2(\mathbf{Z})$ we can do something similar to obtain

$$\Gamma\backslash\mathbf{H}.$$

One of the most prominent examples of such a subgroup is

$$\Gamma(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbf{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\right\}$$

along with

$$\Gamma_1(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbf{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}\right\}$$

$$\Gamma_0(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbf{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}\right\}.$$

$\Gamma(N)$ is normal inside $SL_2(\mathbf{Z})$ and $\Gamma_1(N)$ is normal inside $\Gamma_0(N)$.

The aforementioned equivalence of categories gives us a smooth projective curve for each of these examples.

In fact one can find a smooth projective curve with $\mathbf{Q}$-coefficients realising each of these Riemann surfaces.

For

$$\Gamma_0(N)\backslash\mathbf{H}^*$$

we have the function $j(z)$ from before, but also $j(Nz)$ which is still a function on the quotient now as

$$\begin{aligned} j(N\gamma z) &= j\left(N\frac{az+b}{cz+d}\right) \\ &= j\left(N\frac{az+b}{c'Nz+d}\right) \\ &= j\left(\frac{aNz+bN}{c'Nz+d}\right) \\ &= j\left(\gamma' Nz\right) \\ &= j\left(Nz\right) \end{aligned}$$

We can therefore let

$$g = \prod_{\gamma}(Y - j(\gamma Nz))$$

the product over the cosets of $\Gamma_0(N) \subseteq SL_2(\mathbf{Z})$.

The coefficients of g are meromorphic functions on $X(1) = \mathbf{C}[j]$. So we have

$$g(Y) = F(j(z), Y)$$

and

$$g(j(Nz)) = F(j(z), j(Nz)) = 0$$

then $F(X, Y)$ is irreducible and has integer coefficients.

Then the curve $X_0(N)$ whose function field is

$$\mathbf{Q}[X, Y]/F(X, Y)$$

so $U \subseteq X_0(N)$ is isomorphic to an affine variety defined by

$$F(X, Y) = 0 \setminus \text{singular pts}$$

$$\begin{aligned} \Gamma_0(N)\backslash\mathbf{H} &\to U(\mathbf{C}) \\ z &\mapsto (j(z), j(Nz)) \end{aligned}$$

$j(\gamma z) = z \; \forall z$ iff $\gamma \in SL_2(\mathbf{Z})$.

If for $z = z_1, z_2$ have $(j(z), j(Nz))$ equal then z_1, z_2 are in the same $\Gamma_0(N)$ orbit.

We can do similar for Γ_1 but only over $\mathbf{Q}(\zeta_N)$.

Elliptic curves. Several definitions:

1. Smooth proj. curve genus 1 with a rational point.
2. smooth curve given by Weierstrass eqn.
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
3. Complex torus of dimension 1.

Over **C** at least all are equivalent.

To get the weierstrass equation from the curve we use Riemann-Roch to see that
$$H(1[0]) = 1,\ H(2[0]) = 2,\ H(3[0]) = 3$$
So we call a generator of $H(2[0]) \smallsetminus H([0])$ the function x same for y and $H(3[0])$, now in $H(6[0])$ we have
$$1, x, y, x^2, xy, y^2, x^3$$
so there is a linear relation among these, giving the Weierstrass equation.

To get the equation for a torus we use the Weierstrass $\wp$ function.

5.2 Modular forms (Asra)

Last time we saw the j-function, which was $\mathrm{SL}_2(\mathbf{Z})$-invariant, this is quite a strong condition, and in fact j is pretty much all we get under this condition. So instead we weaken this somewhat to some other variance property.

If $w = f(z)\,\mathrm{d}z$ on **H** and $f(z)$ is meromorphic. $\gamma \in \Gamma$ then
$$f(\gamma z)d(\gamma z) = f(\gamma z)d\left(\frac{az+b}{cz+d}\right)$$
$$= f(\gamma z)\left(\frac{\cdots \mathrm{d}}{(cz+d)^2}\right)$$
so we get a condition
$$f(\gamma z) = (cz+d)^2 f(z)$$
this is how we come to:

Definition 5.2.1 A holomorphic function $f : \mathbf{H} \to \mathbf{C}$ is a **weakly modular** function for Γ of weight k if
$$f(\gamma z) = (cz+d)^k f(z) \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$
◊

Remark 5.2.2 If $-I \in \Gamma$ and k odd
$$f(-z) = -f(-z)$$
so in this setting we only have interesting behaviour for even k.
If Γ is a congruence subgroup of level N we have
$$\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$$
gives you a q-expansion
$$q = e^{2\pi i z}$$

$$f(z) = \sum_{m \in \mathbf{Z}} a_m q^{m/N}.$$

f is holomorphic at ∞ if $a_m = 0$ for $m < 0$.
f is holomorphic at all cusps if $f(\gamma z)(cz+d)^k$ is holomorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbf{Z})$.

Example 5.2.3 Cusps for $\Gamma_0(p)$, we know we have ∞, what is the orbit of this?

$$\gamma \in \Gamma_0(p),\ \gamma = \begin{pmatrix} a & b \\ cp & d \end{pmatrix}$$

$$\gamma\infty = \frac{a}{cp}$$

so anything with a p in the denominator is equivalent to ∞, what about the rest?

$$\gamma 0 = \frac{b}{d},\ \gcd(b,d) = 1,$$

so we have two cusps. □

Definition 5.2.4 Modular forms. A **modular form** is a weakly modular function that is holomorphic at all the cusps. ◊

Example 5.2.5 Eisenstein series

$$G_k(z) = \sum_{m,n \in \mathbf{Z}}{}' \frac{1}{(mz+n)^k}$$

is a modular form of weight $k > 2$ for $\mathrm{SL}_2(\mathbf{Z})$.

$$\lim_{\operatorname{im} z \to \infty} G_k(z) = \lim_{\operatorname{im} z \to \infty} \sum_{m,n \in \mathbf{Z}}{}' \frac{1}{(mz+n)^k} = \sum_{n \in \mathbf{Z}}{}' \frac{1}{n^k} = 2\zeta(k).$$

So here the function does not vanish at 0. □

Definition 5.2.6 Cusp forms. A **cusp form** is a modular form that vanishes at all cusps. ◊

Given a cusp it will be stabilised by some

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$$

call the smallest such h for a given cusp the **width** of the cusp.

Example 5.2.7 Let's find the width of a cusp in $\Gamma_0(qp)$ we have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

so the width of ∞ is 1.
What about $\alpha = 1/p$?

1. Find an element $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ s.t. $\gamma(\infty) = \alpha$.

2. Compute

$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1}$$

3. Find the smallest x such that $\delta(x) = \Gamma_0(pq)$

$$\gamma = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}, \gamma(\infty) = \frac{1}{p}$$

$$\begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -p & 1 \end{pmatrix} = \begin{pmatrix} 1-px & x \\ -p^2 & px+1 \end{pmatrix}$$

□

Example 5.2.8 A cusp form. Let $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$, $g_2(\tau) = 60G_4(\tau)$, $g_3(\tau) = 140G_6(\tau)$ $\Delta(\tau)$ has weight 12 for $\mathrm{SL}_2(\mathbf{Z})$. This vanishes at ∞ because

$$\zeta(4) = \frac{\pi^4}{90}$$

$$\zeta(6) = \frac{\pi^6}{945}$$

also

$$j(z) = \frac{g_2(\tau)^3}{\Delta(\tau)}$$

so $\Delta(\tau)$ vanishes at ∞ because $g_2(\tau)$ doesn't and $j(z)$ has a simple pole at ∞.□

$M_k(\Gamma)$ as the space of modular forms of weight k for Γ is a $\mathbf{C}$ -v.s. $S_k(\Gamma)$ as the space of cusp forms of weight k for Γ is a $\mathbf{C}$ -v.s.

Theorem 5.2.9 *$M_k(\Gamma)$ and $S_k(\Gamma)$ are finite dimensional*

$$\dim(M_k(\Gamma)) = \begin{cases} 0 & \text{if } k \le -1 \\ 1 & \text{if } k = 0 \\ (k-1)(g-1) + v_\infty \frac{k}{2} + \sum_p [\frac{k}{2}(1 - \frac{1}{e_p})] & \text{if } k \ge 2 \end{cases}$$

where g is the genus of $X(\Gamma)$ v_∞ is the number of inequivalent cusps P are the elliptic points $[\cdot]$ is the integer part

$$\dim(S_k(\Gamma)) = \begin{cases} 0 & \text{if } k \le 0 \\ (k-1)(g-1) + v_\infty(\frac{k}{2} - 1) + \sum_p [\frac{k}{2}(1 - \frac{1}{e_p})] & \text{if } k \ge 2 \end{cases}$$

$$\dim(S_2(\Gamma)) = g(X(\Gamma))$$

Proposition 5.2.10 *If $f \in S_2(\Gamma)$ then $f(z)\,\mathrm{d}z$ is a holomorphic differential.*

Given an elliptic curve

$$E/\mathbf{C} = \mathbf{C}/\Lambda$$

$$E \to E'$$

$$\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda',$$

studying degree n isogenies, is like studying index n sublattices

Definition 5.2.11 $n \ge 1$ then $T(n)$ is the nth **Hecke operator** acting on

$$\mathrm{Div}(\mathcal{L})$$

by

$$T(n)\Lambda = \sum_{\Lambda' \subseteq \Lambda, [\Lambda:\Lambda'] = n} (\Lambda')$$

◊

Definition 5.2.12 Let $\lambda \in \mathbf{C}^\times$ the homothety operator R_λ is $R_\lambda \Lambda = \lambda\Lambda$. ◊

Theorem 5.2.13

1.
$$R_\lambda R_\mu = R_{\lambda\mu}$$

2.
$$R_\lambda T(n) = T(n) R_\lambda$$

3.
$$T(nm) = T(n)T(m),\ \gcd(n, m) = 1$$

4.
$$T(p^e)T(p) = T(p^{e+1}) + pT(p^{e-1})R_p$$

Proof. Of 4.

$\Lambda \in \mathcal{L}$ for $\Lambda' \subseteq \Lambda$ index p^{e+1} have

$$a(\Lambda') = \#\{\Gamma : \Lambda' \subseteq \Lambda \subseteq_p \Lambda\}$$

$$b(\Lambda') = 1 \text{ if } \Lambda' \subseteq p\Lambda$$

now

$$T(p^e)T(p)\Lambda = T(p^e)\sum_{\Gamma \subseteq_p \Lambda}(\Gamma) = \sum_{\Gamma \subseteq_p \Lambda}\sum_{\Lambda' \subseteq_{p^e} \Gamma}(\Lambda') = \sum_{\Lambda' \subseteq_{p^e} \Gamma} a(\Lambda')(\Lambda')$$

$$T(p^{e+1})\Lambda = \sum_{\Lambda' \subseteq_{p^{e+1}} \Lambda}(\Lambda')$$

$$T(p^{e-1})R_p\Lambda = T(p^{e-1})(p\Lambda) = \sum_{\Lambda'' \subseteq_{p^{e-1}} p\Lambda}(\Lambda'') = \sum_{\Lambda' \subseteq_{p^{e+1}} \Lambda} b(\Lambda')(\Lambda')$$

Split into cases, do some maths.. ■

Hecke operators on lattices Given $\Lambda' \subseteq_n \Lambda$ there is an integer matrix of determinant n taking one basis to the other. Have a correspondence

$$\{\alpha \in M_2(\mathbf{Z}) : \det(\alpha) = n\} \leftrightarrow \{\Lambda' : \Lambda' \subseteq_n \Lambda\}$$

representatives in Hermite normal form

$$S_n = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n,\ a, d > 0\, 0 \leq b < d\}$$

Corollary 5.2.14 *Let $\Lambda \in \mathcal{L}$, $\Lambda = \mathbf{Z}w_1 + \mathbf{Z}w_2$ then $T(n)$ acts as follows*

$$T(n)\Lambda = \sum_{ad=n,\, a,d>0\, 0\leq b<d} \mathbf{Z}(aw_1 + bw_2) + \mathbf{Z}dw_2 = \sum_{\alpha \in S_n} \alpha\Lambda$$

Corollary 5.2.15 *For p prime $T(p)$:*

$$T(p)\Lambda = \mathbf{Z}pw_1 + \mathbf{Z}w_2 + \sum_{0\leq b<p} \mathbf{Z}(w_1 + bw_2) + \mathbf{Z}pw_2.$$

The Hecke operators act on modular forms $f(\tau)$ by reinterpreting weakly modular functions of weight k as functions on lattices that have a weight k action under homothety.

This boils down to

$$(T_k(n)f)(\tau) = n^{k-1} \sum_{ad=n,\, a,d>0} \sum_{0\leq b<d} d^{-k} f\left(\frac{a\tau+b}{d}\right)$$

Corollary 5.2.16 *For p prime*

$$(T_k(p)f)(\tau) = p^{k-1} f(pz) + \frac{1}{p}\sum_{0\leq b<p} f\left(\frac{z+b}{p}\right).$$

We have an action on fourier expansions

$$f(\psi) = \sum_{m\in\mathbf{Z}} a_m q^m$$

$$\begin{aligned} T_k(p)f(\tau) &= p^{k-1}\sum_{m\in\mathbf{Z}} a_m q^{pm} + \frac{1}{p}\sum_{b=0}^{p-1}\left(\sum_{m\in\mathbf{Z}} a_m e^{2\pi i m(z+b)/p}\right) \\ &= p^{k-1}\sum_{m\in\mathbf{Z}} a_m q^{pm} + \frac{1}{p}\sum_{m\in\mathbf{Z}} a_m e^{2\pi i m z/p}\sum_{b=0}^{p-1}\underbrace{e^{2\pi i m b/p}}_{p \text{ if } p\mid m, 0\text{otw}} \\ &= p^{k-1}\sum_{m\in\mathbf{Z}} a_m q^{pm} + \sum_{m\in\mathbf{Z}} a_{pm} q^m \end{aligned}$$

Corollary 5.2.17

$$a_1(T_p(f)) = a_p(f)$$

If $f \in S_k(\Gamma_0(1))$ is an eigenfunction for these operators we can normalise so that $a_1(f) = 1$.

$$T(m)T(n) = T(mn)$$

$$a_m a_n = a_{mn}$$

$$a_{p^r} = a_p a_{p^{r-1}} + p^{k-1} a_{p^{r+1}}$$

Definition 5.2.18 Petersson inner product. The **Petersson inner product** of two cusp forms $f, g \in S_k(\mathrm{SL}_2(\mathbf{Z}))$ is defined to be

$$\langle f, g\rangle = \int_{\mathcal{D}} f\bar{g}y^{k-2}\,\mathrm{d}x\,\mathrm{d}y$$

where $\mathcal{D}$ is a fundamental domain for $\mathrm{SL}_2(\mathbf{Z})$. ◊

Proposition 5.2.19 *Let $f, g \in S_k(\mathrm{SL}_2(\mathbf{Z}))$, $n \in \mathbf{N}$ then*

$$\langle T(n)f, g\rangle = \langle f, T(n)g\rangle.$$

5.3 Abelian varieties and Jacobians (Angus)

5.3.1 Background

Definition 5.3.1 An elliptic curve is any one of the following

1. Smooth projective curve of genus 1 with a marked rational point.
2. A smooth projective curve with a group law
3. if $k \subseteq \mathbf{C}$ we have
$$E(\mathbf{C}) = \mathbf{C}/\Lambda$$
$$\Lambda = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2,\ \omega_1/\omega_2 \notin \mathbf{R}$$
4. if char $k \neq 2, 3$ A smooth projective curve specified by
$$y^2 = x^3 + ax + b.$$

◊

Aash showed that 1 implies 4 and 3 implies 1.

One can view the group law on E either via the chord-tangent method (Bezout's theorem). Or via the isomorphism

$$E \longrightarrow \mathrm{Pic}^0(E)$$
$$P \mapsto [P] - [0].$$

Definition 5.3.2 An abelian variety is a proper irreducible variety with a group law given by regular functions. ◊

Remark 5.3.3

1. In this definition proper is equivalent to projective.
2. The rigidity theorem tells us:
   (a) Any morphism of abelian varieties that preserves the identity is a homomorphism.
   (b) Abelian varieties are abelian

5.3.2 Ablelian varieties over C

Proposition 5.3.4 *Let $A/k \subseteq \mathbf{C}$ then*

$$A(\mathbf{C}) = \mathbf{C}^g/\Lambda$$

where $g = \dim A$ and $\Lambda \subseteq \mathbf{C}^g$ is a rank $2g$ lattice.

Proof. The lie algebra $\mathrm{Lie}(A(\mathbf{C}))$ is a complex vector space of dimension g. We have the exponential

$$\exp\colon \mathrm{Lie}(A(\mathbf{C})) \longrightarrow A(\mathbf{C})$$

which is surjective onto the connected component of the identity, and locally at 0 a diffeomorphism. So exp surjects. Since its locally isomorphic at 0 we have ker(exp) discrete and hence a lattice. A proper means $A(\mathbf{C})$ is compact so

$$\mathrm{rank}\ker(\exp) = 2g.$$ ∎

We have a map

$$\{\mathrm{AVs}/\mathbf{C}\} \longrightarrow \{\text{complex tori}\}$$

but this is not surjective. Which lattices give AVs?

Definition 5.3.5 Let V be a $\mathbf{C}$-vector space and $\Lambda \subseteq V$ be a full lattice. A **Hermitian form** on V is a function

$$H\colon V \times V \to \mathbf{C}$$

which is $\mathbf{C}$-linear in the first component, $\mathbf{C}$-antilinear in the second (i.e. a sesquilinear form). And satisfies

$$H(u,v) = \overline{H(v,u)}$$

A Riemann form on (V,Λ) is a positive definite Hermitian form on V s.t. $\mathrm{im}(H|_V)\colon \Lambda \to \mathbf{Z}$. ◊

Proposition 5.3.6 *We have a bijection*

$$\{AVs/\mathbf{C}\} \leftrightarrow \{(V,\Lambda) \text{ s.t. there is a Riemann form on } (V,\Lambda)\}.$$

Proof. Swinnerton-Dyer analytic theory of AVs ch.2. ■

Example 5.3.7 For an elliptic curve $E(\mathbf{C}) = \mathbf{C}/\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$

$$H(u,v) = u\bar{v}/\mathrm{im}(\omega_1\bar{\omega}_2).$$

□

5.3.3 Jacobian varieties

Definition 5.3.8 Given X a curve

$$\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\{(f) : f \in K(X)\}$$

this is some abelian group. ◊

Theorem 5.3.9 *Let X be a genus g curve $/k$. Then there exists an abelian variety* $\mathrm{Jac}(X)/k$ *of* $\dim = g$ *s.t.*

$$\mathrm{Jac}(X)(L) = \mathrm{Pic}^0(X \otimes L)$$

Remark 5.3.10 This is false as stated unless $X(k) \neq \emptyset$.

Proof. Idea: Pick $P_0 \in X(k)$ we have a bijection

$$\mathrm{Div}^0(X) \to \mathrm{Div}^r(X)$$

$$D \mapsto D + r[P_0]$$

we have a map

$$X^r \to X^r/S_r = X^{(r)} \to \mathrm{Div}^r(X)$$

we can construct $\mathrm{Jac}(X)$ as a quotient of $X^{(r)}$ full details Milne AVs ch. 2. ■

Jacobians over C. Given X a compact Riemann surface of genus g then

$$H^0(X,\Omega^1_X) \simeq \mathbf{C}^g$$

one might wish to consider, for $P, Q \in X$, $\omega \in H^0(X,\Omega^1_X)$

$$\int_P^Q \omega$$

this is not well defined as there are choices of path $P \to Q$.

$$H_1(X, \mathbf{Z}) = \mathbf{Z}^{2g}$$

have a map

$$H_1(X, \mathbf{Z}) \to H^0(X, \Omega^1_X)^\vee$$
$$\gamma \mapsto (\omega \mapsto \int_\gamma \omega)$$

Let

$$J(X) = H^0(X, \Omega^1_X)^\vee / H_1(X, \mathbf{Z})$$

Theorem 5.3.11 *$J(X)$ is the $\mathbf{C}$ points of an abelian variety over $\mathbf{C}$. Further the map*

$$\mathrm{Pic}^0(X) \to J(X)$$
$$[P] - [Q] \mapsto (\omega \mapsto \int_Q^P \omega)$$

is an isomorphism of abelian groups.

Proof. For the first claim we need a Riemann form on

$$(H^0(X, \Omega^1_X)^\vee, H_1(X, \mathbf{Z}))$$

we have

$$H_1(X, \mathbf{Z}) \times H_1(X, \mathbf{Z}) \to \mathbf{Z}$$
$$(\gamma_1, \gamma_2) \mapsto -(\gamma_1 \cap \gamma_2).$$

∎

Remark 5.3.12 In this case we see

$$\mathrm{Lie}(\mathrm{Jac}(X)) = H^0(X, \Omega^1_X)$$

this is true in general.

5.3.4 Some constructions/properties of AVs

Let A, B be AVs$/k$. Any identity preserving morphism $\phi \colon A \to B$ is a homomorphism. Such a homomorphism is called an isogeny if it surjective with finite kernel. i.e. $[n] \colon A \to A$ is an isogeny and for $\mathrm{char}(k) \nmid n$.

$$A[n] \simeq (\mathbf{Z}/n)^{2g}$$

then we have the Tate module for l prime

$$T_l A = \varprojlim_n A[l^n] \simeq \mathbf{Z}_l^{2g}$$

in fact

$$H^1_{\mathrm{et}}(A, \mathbf{Z}_l) \simeq T_l A^\vee$$

we can also consider $\mathrm{Pic}^0(A)$. There exists an abelian variety

$$\hat{A}/l$$

s.t.

$$\hat{A}(L) = \mathrm{Pic}^0(A \otimes L)$$

this is called the dual abelian variety. So earlier we saw $\hat{E} \simeq E$. in general $\hat{A} \not\simeq A$.

However for an ample divisor D we get an isog

$$\phi_D : A \to \hat{A}$$

$$P \mapsto t_P^* D - D$$

an isogeny $\phi : A \to \hat{A}$ is a polarization if

$$\phi = \phi_D / \bar{k}$$

over $\mathbf{C}$ a polarization is equivalent to a choice of Riemann form.

A principal polarization is a polarization which is an isomorphism. e.g.

$$\phi_{[0]} : E \to \hat{E}$$

$$P \mapsto [P] - [0]$$

Remark 5.3.13 Jacobian varieties always admit principal polarizations.

On $T_l A$ we have a Weil pairing

$$T_l A \times T_l A^\vee \to \mathbf{Z}_l$$

Maps between Jacobians. Let $X, Y/k$ be curves and $f : X \to Y$ a morphism.

Definition 5.3.14 We have a pushforward map

$$f_* : \operatorname{Pic}^0(X) \to \operatorname{Pic}^0(Y)$$

$$\sum n_x[x] \mapsto \sum n_x[f(x)]$$

if f is finite then we have a pullback

$$f^* : \operatorname{Pic}^0(Y) \to \operatorname{Pic}^0(X)$$

$$\sum n_y[y] \mapsto \sum n_y[f^{-1}(y)]$$

(with multiplicity). ◊

We want further maps between jacobians

Definition 5.3.15 A correspondence between X, Y is a curve Z and a pair of finite morphisms.

$$X \leftarrow Z \rightarrow Y$$

then we get induced maps

$$T_* = g_* f^* : \operatorname{Pic}^0(X) \to \operatorname{Pic}^0(Y)$$

$$T^* = f_* g^* : \operatorname{Pic}^0(Y) \to \operatorname{Pic}^0(X)$$

◊

Modular jacobians and Hecke correspondences. Consider $p \nmid N$ we have

$$X_0(N) = \{(E, C_N) : E \text{ e.c. }, C_N \text{ cyclic sub order } N\}$$

$$X_0(pN) = \{(E, C_{pN})\} = \{(E, C_N, C_p)\}$$

so we have

Definition 5.3.16 the Hecke correspondence T_p on $X_0(N)$ is

$$X_0(N) \leftarrow X_0(pN) \rightarrow X_0(N)$$
$$(E, C_N) \leftarrow (E, C_N, C_p) \rightarrow (E/C_p, C_p + C_N).$$

◊

We have the modular jacobian $J_0(N)$ and the induced map

$$T_p : J_0(N) \rightarrow J_0(N)$$
$$[E] \mapsto \sum_{C_p \subseteq E} [E/C_p]$$

One can consider $J_0(N)_{\mathbf{F}_p}$

Theorem 5.3.17 Eichler-Shimura. $T_{p*} = \mathrm{Frob}_p + p\,\mathrm{Frob}_p^{-1} \in \mathrm{End}(J_0(N)_{\mathbf{F}_p})$.

5.4 Ricky Show

5.4.1 Moduli of PPAVs

Recall if $A/\mathbf{C}$ is an abelian variety, then

$$A = A(\mathbf{C}) = \mathbf{C}^g/\Lambda,\ g = \dim(A)$$
$$\Lambda \cong H_1(A, \mathbf{Z})$$

Also a polarization $\lambda : A \rightarrow A^\vee$ is equivalent to choosing a Riemann form

$$E : \Lambda \times \Lambda \rightarrow \mathbf{Z}$$

s.t.

1. E is bilinear alternating
2. $E_{\mathbf{R}} : V \times V \rightarrow \mathbf{R}$ has $E_{\mathbf{R}}(iv, iw) = E_{\mathbf{R}}(v, w)$.
3. $$H(v, w) = E_{\mathbf{R}}(iv, w) + iE_{\mathbf{R}}(v, w)$$
   is a positive definite Hermitian form on V.

A principal polarization corresponds to E being a perfect pairing.

Definition 5.4.1 A PPAV (principally polarized abelian variety) is a pair (A, λ).
◊

If $(\mathbf{Z}^{2g}, \Psi)$ is the standard $2g$-dim symplectic form Ψ then by linear algebra there is a symplectic isomorphism

$$\alpha : \mathbf{Z}^{2g} \xrightarrow{\sim} \Lambda$$

with $\Psi(v, w) = E(\alpha(v), \alpha(w))$.

Recall the standard Ψ is

$$\Psi(v, w) = v^{\mathrm{T}} J w,\ J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$$

Definition 5.4.2 The **Siegel upper half space** is

$$\mathscr{H}_g = \{Z = X + iY \in M_g(\mathbf{C}) : Z^{\mathrm{T}} = Z;\ X, Y \in M_g(\mathbf{R});\ Y > 0\}$$

i.e. Y is pos. def. ◊

Check: $\mathscr{H}_1$ is the usual upper half plane.

Proposition 5.4.3 *$\mathscr{H}_g \cong \mathrm{Sp}_{2g}(\mathbf{R})/U(g)$ where $\mathrm{Sp}_{2g}(R) = \{M \in \mathrm{GL}_{2g}(R) : M^{\mathrm{T}} J M = J\}$*

$$U(g) = O(2g) \cap \mathrm{Sp}_{2g}(\mathbf{R}) \cap \mathrm{GL}_g(\mathbf{C}).$$

Proof. (Sketch) First one can show that $\mathrm{Sp}_{2g}(\mathbf{R})$ acts transitively on $\mathscr{H}_g$ via linear fractional transformations:

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbf{R}),\ Z \in \mathscr{H}_g$$

$$M \cdot Z = (AZ + B)(CZ + D)^{-1} \in \mathscr{H}_g$$

second one computes Stab $J = U(g)$

For $g = 1$, $\mathrm{Sp}_2(\mathbf{R}) = \mathrm{SL}_2(\mathbf{R})$ acts transitively on $\mathscr{H}_1$, $\mathrm{Stab}(i) = \mathrm{SO}(2) = U(1)$.

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} i = i$$

and if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} i = i$$

then $ai + b = -c + di$ so $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{SO}(2)$. ∎

Proposition 5.4.4 *There is a natural bijection between*

$$\{(A, \lambda, \alpha) : (A, \lambda) = PPAV,\ \alpha\colon \mathbf{Z}^{2g} \xrightarrow{\sim} \Lambda\} \xrightarrow{\sim} \mathscr{H}_g$$

this induces a bijection

$$\{(A, \lambda)\} \xrightarrow{\sim} \mathrm{Sp}_{2g}(\mathbf{Z})\backslash\mathscr{H}_g = \mathrm{Sp}_{2g}(\mathbf{Z})\backslash \mathrm{Sp}_{2g}(\mathbf{R})/U(g).$$

Proof. We will construct a map

$$\{(A, \lambda, \alpha)\} \xrightarrow{\sim} \mathrm{Sp}_{2g}(\mathbf{R})/U(g)$$

first we construct a bijection between

$$\{(A, \lambda, \alpha)\}$$

and some linear data on a fixed space , so given (A, λ, α) use α to identify

$$\alpha\colon \mathbf{Z}^{2g} \xrightarrow{\sim} \Lambda = H_1(A, \mathbf{Z})$$

then tensor with $\mathbf{R}$ to get

$$\alpha_{\mathbf{R}}\colon \mathbf{R}^{2g} \xrightarrow{\sim} \Lambda \otimes \mathbf{R} \cong \mathrm{Lie}(A)(= \mathbf{C}^g)$$

the action of i on the right induces J on the left with $J^2 = -I$.

From $E_{\mathbf{R}}(iv, iw) = E_{\mathbf{R}}(v, w)$ we get J symplectic

$$\Psi_{\mathbf{R}}(Jv, Jw) = \Psi_{\mathbf{R}}(v, w)$$

from $E_{\mathbf{R}}(iv, v) > 0$ we get J is positive

$$\Psi_{\mathbf{R}}(Jv, v) > 0$$

conversely given J symplectic positive $J^2 = -I$ on $\mathbf{R}^{2g}$ we can construct $(A, \lambda) = (V/\mathbf{Z}^{2g}, E)$ This comes with an α for free since $H_1(A, \mathbf{Z}) \cong \mathbf{Z}^{2g}$.

Suppose J and J_0 are two complex structures, symplectic positive matrices on $\mathbf{R}^{2g}$. Then a lemma from linear algebra tells us that there exists a $S \in \mathrm{Sp}_{2g}(\mathbf{R})$. s.t. $J_0 = SJS^{-1}$. We see that this S is well defined up to an element of $G = Z(J) \cap \mathrm{Sp}_{2g}(\mathbf{R})$. But if $\gamma \in G$ then γ preserves the associated $\mathbf{C}$-str. on $\mathbf{R}^{2g}$. then since γ is symplectic, it preserves

$$H(v, w) = E_{\mathbf{R}}(iv, w) + iE_{\mathbf{R}}(v, w)$$

implies

$$\gamma \in U(g). \qquad \blacksquare$$

5.4.2 Hodge structures

Let M be a C^∞ compact $\mathbf{R}$-manifold. Then $H^i_{\text{sing}}(M, \mathbf{R}) \cong H^i_{\text{dR}}(M)$. What about for compact $\mathbf{C}$-manifolds X? For M have $H^i_{\text{dR}}(M) = H^i(\Omega^\bullet(M))$. This won't give de Rham isomorphism for X:

$$H^i_{\text{sing}}(X)$$

supported up to $i = 2d$ with $d = \dim_{\mathbf{C}}(X)$. but $H^i(\Omega^\bullet_{\text{hol}}(C))$ is supported up to $i = d$.

For M

$$0 \to \underline{\mathbf{R}} \to \Omega^0 \to \Omega^1 \to \cdots \to \Omega^d \to 0$$

is a resolution of $\underline{\mathbf{R}}$ by acyclic sheaves, by the existence of C^∞ bump functions.

$$H^i_{\text{dR}}(M) \cong H^i(M, \underline{\mathbf{R}}) \cong H^i_{\text{sing}}(M, \mathbf{R}).$$

For X this doesn't work with $\Omega^\bullet_{\text{hol}}$ as there are no holomorphic bump functions.

$$0 \to \underline{\mathbf{C}} \to \Omega^0_{\text{hol}} \to \Omega^1_{\text{hol}} \to \cdots \to \Omega^\bullet_{\text{hol}} \to 0$$

is still a resolution but not acyclic. Instead we use hypercohomology which takes as input any resolution and outputs a cohomology group. This has the property that

$$H^i(X, \underline{\mathbf{C}}) \cong \mathbf{H}^i(\Omega^\bullet_X)$$

so we define $H^i_{\text{dR}}(X) = \mathbf{H}^i(\Omega^\bullet_X)$. so that

$$H^i_{\text{dR}}(X) \cong H^i(X, \underline{\mathbf{C}}) \cong H^i_{\text{sing}}(X, \mathbf{C})$$

On X we have the sheaf of (p, q) forms $\Omega^{p,q}$ These are locally given by

$$\sum_{|I|=p,|J|=q} f_{I,J}\, \mathrm{d}z_I\, \mathrm{d}\bar{z}_J.$$

We have

$$\bar{\partial}\colon \Omega^{p,q} \to \Omega^{p,q+1}$$

satisfying $\bar{\partial}^2 = 0$. So we can define $H^{p,q}(X) = \ker \bar{\partial}/\mathrm{im}\, \bar{\partial}$ (Dolbeaut cohomology).

Theorem 5.4.5 Hodge decomposition. *For a compact Kahler manifold (e.g. X a projective variety) we have*

$$H^n_{\mathrm{dR}}(X) \cong \bigoplus_{p+q=n} H^{p,q}(X).$$

Remark 5.4.6

$$H^{p,q}(X) \cong H^q(X, \Omega^p)$$

using $\bar{\partial}$ Poincaré lemma

Example 5.4.7 $E/\mathbf{C}$ elliptic curve.

$$H^0_{\mathrm{dR}} = H^{0,0}$$

$$H^1_{\mathrm{dR}} = H^{1,0} \oplus H^{0,1}$$

$$H^2_{\mathrm{dR}} = H^{2,0} \oplus H^{1,1} \oplus H^{0,2}$$

outer terms 0, diamond is 1 , 1 , 1, 1. □

Definition 5.4.8 Hodge structures. A **Hodge structure** on $V/\mathbf{R}$ is a $\mathbf{Z}$-bigrading on $V_{\mathbf{C}} = V \otimes \mathbf{C}$ such that

$$\overline{V}^{p,q} = V^{q,p}$$

its of **Hodge type** $S \subseteq \mathbf{Z}^2$ if $V^{pq} \neq 0$ iff $(p,q) \in S$, ◊

Example 5.4.9 the Hodge decomposition gives a hodge structure on $H^n_{\mathrm{sing}}(X, \mathbf{R})$. □

If V has a hodge structure of weight n (i.e. $V^{pq} \neq 0$ iff $p, q = n$). Then we can recover the hodge structure from the associated hodge filtration

$$\mathrm{Fil}^p\, V_{\mathbf{C}} = \bigoplus_{p' \geq p} V^{p'q}$$

Example 5.4.10

$$\mathrm{Fil}^0(H^1(E)) = H^{1,0} \oplus H^{0,1}$$

$$\mathrm{Fil}^1(H^1(E)) = H^{1,0}$$

$$\mathrm{Fil}^2(H^1(E)) = 0$$

□

Exercise 5.4.11

$$V^{p,q} = \mathrm{Fil}^p\, V \cap \overline{\mathrm{Fil}^q\, V}$$

in weight n.

Alternative definition.

$$\mathbf{S} = \mathrm{Res}^{\mathbf{C}}_{\mathbf{R}} \mathbf{G}_m$$

$$\mathbf{S}(A) = \{(a, b) \in A^2 : a^2 + b^2 \neq 0\}$$

$$\mathbf{S}(\mathbf{R}) = \mathbf{C}^\times$$

Proposition 5.4.12 *There is a natural bijection between morphisms of algebraic groups*

$$\mathbf{S} \to \mathrm{GL}(V)$$

and Hodge structures on V.

Hence for any lie group G we can define a hodge structure on G as a morphism of algebraic groups

$$\mathbf{S} \to G$$

If $G \to \mathrm{GL}(V)$ is a faithful rep this induces a hodge structure on V.

Definition 5.4.13 A polarization of a HS $h\colon \mathbf{S} \to \mathrm{GL}(v)$ is an alternating bilinear form

$$\Psi\colon V \times V \to \mathbf{R}$$

with

1. $$\Psi(Jv, Jw) = \Psi(v, w) \text{ for } J = h(i)$$

2. $$\Psi(v, Jw) \text{ is pos. def.}$$

◊

5.5 Variations of Hodge Structures

5.5.1 Review of Hodge Theory

X complex manifold $X \subseteq \mathbf{P}^N$ which is m-dimensional. For each n associate to X

$$H_{\mathbf{Z}} = H^n_{\mathrm{sing}}(X, \mathbf{Z})/\mathrm{tors}$$
$$H_{\mathbf{C}} = H_{\mathbf{Z}} \otimes \mathbf{C} = H^n_{\mathrm{dR}}(X)$$

we have a bilinear pairing

$$Q\colon H_{\mathbf{Z}} \times H_{\mathbf{Z}} \to \mathbf{Z}$$
$$Q(\alpha, \beta) = \int_X \alpha \cup \beta \cup \omega^{m-n}$$

where ω is a generator of $H^2(\mathbf{P}^N, \mathbf{Z})$ restricted to X. This gives us the set-up of X as a differentiable manifold. Now say something about complex structure. We have a decomposition of differential forms on X

$$A^n(X) = \bigoplus_{p+q=n} A^{p,q}$$

degree n forms decomposing as a combination of type p, q forms.

Hodge theorem descends to a decomposition on cohomology

$$H^n_{\mathrm{dR}}(X) = \bigoplus_{p+q=n} H^{p,q}$$

$$H^{p,q} = \overline{H^{q,p}}$$
$$Q(H^{p,q}, H^{p',q'}) = 0$$

unless $p + p' = q + q' = n$.

A hodge structure of weight n is the data $(H_{\mathbf{Z}}, Q)$ satisfying the Hodge decomposition, Bilinearity

Questions:

1. To what extent does the HS of X determine X? (Torelli problem)
2. To what extent can we read off the geometric data of X from its Hodge structure.

5.5.2 Variations of Hodge structures:

Let $Y \subseteq X$ be codimension k, this gives a class in

$$H^{k,k}(X) \subseteq H^{2k}(X, \mathbf{C})$$

what about the converse?

For each cohomology class γ in $H^{2k}(X, \mathbf{C})$ is γ a rational linear combination of classes of subvarieties. (Hodge conjecture).

5.5.2.1 Hodge theory for curves

$(H_{\mathbf{Z}}, Q)$, $H^{1,0} \oplus H^{0,1}$ have the period matrix

$$H^{0,1}/\Lambda \cong \mathrm{Jac}(C)$$

$$y^2 = x(x-1)(x-\lambda)$$
$$\lambda \in \mathbf{P}^1 - \{0, 1, \infty\}$$

each $E_\lambda \leftrightarrow H^{1,0} \oplus H^{0,1}$ so can ask as λ varies we can ask how $H^{1,0}$ is situated inside of $H^{1,0} \oplus H^{0,1}$.

$$\omega = \frac{\mathrm{d}x}{y} \in H^0(X, \Omega_X)$$

pairing with $H_1(X)$

$$\int_\gamma \omega.$$

For B a variety $\{X_b\}$ are varieties with Hodge structures for each $b \in B$. Locally we can identify

$$H_{\mathbf{Z}} = H^n(X_b, \mathbf{Z})/\mathrm{tors}$$

and $H_{\mathbf{C}}$ with that of X_{b_0}.

Then consider

$$H^{n-k,k}(X_b)$$

or the associated

$$F^k = \bigoplus_{l=0}^{k} H^{n-l,l}(X_b)$$

subspaces of $H_{\mathbf{C}}$.

Question: What is a moduli space of linear subspaces?

Answer: The grassmanian!

$$\mathrm{Gr}(k, V)$$

of k-dimensional subspaces of a fixed vector space V. What is the tangent space to the Grassmanian at a point $W \subseteq V$?

$$\mathrm{Hom}(W, V/W)$$

if we take the complementary subspace $W \oplus C = V$ given another subspace

$$W' \cap C = \{0\}$$

have $\pi_{W'}, \pi_C$

$$\mathrm{Gr}(k, V) = \{\text{all } W'\}$$
$$\cong \mathrm{Hom}(W, C)$$

by $\pi_C \circ (\pi_W|_{W'})^{-1}$.

Fact 5.5.1

1. *$\phi\colon B \to \mathrm{Gr}$ mapping $b \mapsto F^k(X_b) \subseteq H_{\mathbf{C}}$ is holomorphic.*
2. *In terms of identifying the tangent space of the grassmanian to the hom set, the image under*
$$d\phi_k = \delta_k$$
of any tangent vector of B at b_0 carries F^k to F^{k+1}/F^k so we have maps
$$\delta_k\colon T_{b_0}B \to \mathrm{Hom}(H^{n-k,k}(X), H^{n-k-1,k+1}(X))$$
satisfying
$$\delta_{k+1}(V) \circ \delta_k(W) = \delta_{k+1}(W) \circ \delta_k(W)$$
for all $v, w \in T$.

Since $F^k(X_b)$ satisfy
$$Q(F^k, F^{n-k-1}) = 0$$
for all b.
$$Q(\delta_v(v)(\alpha), \beta) + Q(\alpha, \delta_{n-k-1}(v)(\beta)) = 0$$
for all $\alpha \in H^{n-k,k}(X)$, $\beta \in H^{k+1,n-k-1}(X)$ for $v \in T$

Definition 5.5.2 An **infinitesimal variation of Hodge structures** is
$$(H_{\mathbf{Z}}, Q, H^{p,q}, T, \delta_q\colon T \to \mathrm{Hom}(H^{p,q}, H^{p-1,q+1}))$$
◊

Two observations:

Remark 5.5.3 Variations of hodge structures are often computable, e.g. for hypersurfaces in $\mathbf{P}^N$.
$$X \subseteq \mathbf{P}^{n+1}$$
let $X = \{f = 0\}$ of deg d.

Lefschetz implies the only interesting cohomology is in the middle dimension.
$$H^n(X)$$
$$H^{n,0}(X)$$
Poincaré residues of $n+1$ forms of $\mathbf{P}^{n+1}$ with poles along X
$$\frac{\mathrm{Res}_\omega\, g(z_0, \ldots, z_{n+1})\Omega}{f} = \frac{g\widetilde{\Omega}}{\sum \frac{\partial f}{\partial z_i}}.$$
$$\mathbf{C}[z_0, \ldots, z_{n+1}]/\text{Jacobian ideal}$$
graded parts $H^{p,q}(X)$

Problem 5.5.4 Identify $H_{\mathbf{Z}}$ inside of H^n □

Solution: VHS δ_k maps turn out to be polynomial multiplication $d \geq n+1$.

Theorem 5.5.5 Noether-Lefschetz. *A surface $S \subseteq \mathbf{P}^4$ of degree $d \geq 4$ having general moduli contains no curves other than complete intersections $S \cap T$ with other surfaces T.*

5.6 Moduli of linearized C-structures (RICKY)

5.6.1 Motivation: Period morphisms

Recall for A a polarized AV we get a lattice $H_1(A, \mathbf{Z})$ with some structure. To keep track of the $\mathbf{C}$-structure we record the Hodge structure induced on $H_1(A, \mathbf{R})$ via the Hodge decomposition theorem. If we want to say construct a moduli space of Elliptic Curves we might try to create a moduli space of $\mathbf{C}$-structures on a fixed torus T.

The linearized version of this is to fix $H^1(T, \mathbf{R})$ and consider possible Hodge structures on it.

Example 5.6.1

$$E_\lambda \colon y^2 = x(x-1)(x-\lambda)$$

$$\mathcal{E} \xrightarrow{f} S = \mathbf{P}^1 \setminus \{0, 1, \infty\}$$

then we can identify

$$V_\lambda = H^1_{\mathrm{sing}}(E_\lambda, \mathbf{R})$$

for nearby $\lambda \in S$. Then the Hodge structure looks like:

$$F^1 V_{\lambda,\mathbf{C}} = \langle \frac{\mathrm{d}x}{y} \rangle \hookrightarrow V_{\lambda,\mathbf{C}}$$

this induces a period map

$$S \supseteq U \to PP^1$$

sending $s \mapsto F^1 V_{s,\mathbf{C}}$. □

Today generalise the role of $\mathbf{P}^1$ in this.

5.6.2 Moduli of Hodge structures

Recall: a Hodge structure on a real vector space V is equivalent to a morphism $h \colon \mathbf{S} \to \mathrm{GL}(V)$ where $\mathbf{S} = \mathrm{Res}^{\mathbf{C}}_{\mathbf{R}} \mathbf{G}_m$ Given h, let

$$V^{p,q} = \{v \in V_{\mathbf{C}} : h(z)v = z^{-p}\bar{z}^{-q}v\}$$

(the characters of $\mathbf{S}$ are of the form $\chi_{p,q} = z^{-p}\bar{z}^{-q}$ for $(p,q) \in \mathbf{Z}^2$. So a general Hodge structure on a Lie group G is defined to be a map $\mathbf{S} \to G$.

Lemma 5.6.2 *The combinatorial data of two Hodge structures are the same iff they are conjugate (i.e. the maps $\mathbf{S} \to \mathrm{GL}(V)$ are conjugate).*

Proof. If h and h' are conjugate by g then conjugation by g takes $V^{p,q}$ of one into the other (b/c it preserves the character spaces of $\mathbf{S}$). Conversely if $\{V_1^{p,q}, V_2^{p,q}\}$ are two HS with the same combinatorial data then we can take $g \colon V_{\mathbf{C}} \to V_{\mathbf{C}}$. Taking $V_1^{p,q} \cong V_2^{p,q}$ and satisfying $g(\bar{v}) = \overline{g(v)}$ (using Hodge symmetry) since g commutes with $\bar{\cdot}$, it descends to a map on V. ■

Let X be a conjugacy class of morphisms $h \colon \mathbf{S} \to G$.
Impose the condition that:

$$h(\mathbf{R}^\times) \text{ lies in the center of } G(\mathbf{R}) \forall h \tag{5.6.1}$$

(If the HS on V is of weight k then $h(t) = t^k I$, the converse is also true.)

G acts transitively on X (via conjugation). So

$$X = G/K$$

for $K = \mathrm{Stab}(h)$ for some h in X. This gives X the structure of a C^∞-manifold.

The C-strucutre on X. We give $T_h X = \mathrm{Lie}\, G/\mathrm{Lie}\, K$ a $\mathbf{C}$-v.s. structure let $\psi_g(x) = gxg^{-1}$ gives

$$G \longrightarrow \mathrm{Aut}(G)$$

and its derivative is the adjoint map ad. If we compose with $h\colon \mathbf{S} \to G$ we get a hodge structure on $L = \mathrm{Lie}\, G$.

As $h(\mathbf{R}^\times)$ is in the center of $G(\mathbf{R})$, have ad $h(\mathbf{R}^\times)$ is the identity on L. Hence the hodge structure on L is of weight 0. By above remark.

Let $L^{0,0} = L^{0,0}_{\mathbf{C}} \cap L$ be the real $(0,0)$ part of the HS on L.

Lemma 5.6.3

$$L^{0,0} = \mathrm{Lie}\, K$$

Proof. By the definition of K, $\psi_h(k) = k$ for all $k \in K$. Differentiating gives

$$(\mathrm{ad}\, h)(v) = v$$

for all $v \in \mathrm{Lie}\, K$ So $\mathrm{Lie}\, K \subseteq L^{0,0}$. Conversely if $v \in L^{0,0}$ then $(\mathrm{ad}\, h)(v) = v$ implies

$$(\mathrm{ad}\, h)(\exp v) = \exp v$$

so $\exp v \in K$ i.e. $v \in \mathrm{Lie}\, K$. ∎

Lemma 5.6.4 *The inclusion $L \hookrightarrow L_{\mathbf{C}}$ induces an isomorphism of* $\mathbf{R}$*-v.s.*

$$L/L^{0,0} \xrightarrow{\sim} L_{\mathbf{C}}/F^0 L_{\mathbf{C}}.$$

Proof. see notes. ∎

These lemmas combined give $T_h X$ a $\mathbf{C}$-structure.

To get a $\mathbf{C}$-manifold structure on X we embed X into a $\mathbf{C}$ manifold in a way that respects the $\mathbf{C}$-structures on the tangent spaces.

Pick a faithful representation $G \hookrightarrow \mathrm{GL}(V)$. Then $h \in X$ we get a Hodge structure on V via

$$\mathbf{S} \xrightarrow{h} G \xrightarrow{\rho} \mathrm{GL}(V)$$

all other $h' \in X$ have the same combinatorial data.

Let $\mathbf{F}$ be the flag variety parameterises filtrations of the type associated to $h \in X$.

To be safe assume V of weight k.

We have an injective map

$$X \hookrightarrow \phi\mathcal{F}$$

this induces a complex structure on X, see notes for deets.

5.6.3 Geometric conditions and chill (on VHS)

Recall that a VHS parameterised by a space S must satisfy "Griffiths transversality", this translates to the condition

Theorem 5.6.5 *A VHS on V satisfies Griffiths transversality iff*

$$\text{the HS on } L = \mathrm{Lie}(G) \text{ of type } \{(-1,1),(0,0),(1,-1)\}. \tag{5.6.2}$$

Background on Cartan involutions.

Definition 5.6.6 Let G be a real algebraic group with involution σ. The **real form** associated to σ is

$$G^{\sigma}(A) = \{g \in G(A \otimes \mathbf{C}) : \sigma(g) = \bar{g}\}$$

for all $\mathbf{R}$-algebras A. ◊

Example 5.6.7 $G = \mathrm{GL}_n$, $\sigma(g) = (g^{\perp})^{-1}$ then

$$G^{\sigma} = U(n)$$

observe that this is compact! □

Definition 5.6.8 σ is called a **Cartan involution** if G^{σ} is compact, i.e. $G^{\sigma}(\mathbf{R})$ is compact and meets every connected component of $G^{\sigma}(\mathbf{C})$. ◊

Theorem 5.6.9 *Let G be connected, then G is reductive iff G admits a Cartan involution.*

Lemma 5.6.10 for next time. *If K is a compact lie group then any $\mathbf{C}$-representation V of it admits a K-invariant pos. def. Hermitian form*
Conversely if K has a faithful representation admitting a K-inv pos. def. Herm. form. then K is compact.

Proof. K compact, take any $H_0(u,v)$ a pos. def. herm. form on V. Then

$$H(u,v) = \int_K H_0(Ku, Kv)\,\mathrm{d}K$$

is K-invariant with some properties. For the converse statement the conditions imply $K \hookrightarrow U(K)$ hence K is compact. ■

Remark 5.6.11 One source of involutions on G come from $C \in G \setminus Z$ s.t. $C^2 \in Z$ then

$$g \mapsto CgC^{-1}$$

is such an involution. e.g. J!!

References

Bibliography

[1] Balakrishnan, Jennifer S., Robert W. Bradshaw, and Kiran S. Kedlaya. *Explicit Coleman Integration for Hyperelliptic Curves*. In ANTS, pp. 16-31. 2010.

[2] Balakrishnan, Jennifer S. *Coleman integration for even-degree models of hyperelliptic curves*. LMS Journal of Computation and Mathematics 18.1 (2015): 258-265.

[3] Balakrishnan, Jennifer S. *Iterated Coleman integration for hyperelliptic curves*. The Open Book Series 1.1 (2013): 41-61.

[4] Balakrishnan JS, Dogra N. *Quadratic Chabauty and rational points I: p-adic heights*. arXiv preprint arXiv:1601.00388. 2016 Jan 4.

[5] Balakrishnan JS, Dogra N, Müller JS, Tuitman J, Vonk J. *Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level 13*. arXiv preprint arXiv:1711.05846. 2017 Nov 15.

[6] Balakrishnan JS, Tuitman J. *Explicit Coleman integration for curves*. arXiv preprint arXiv:1710.01673. 2017 Oct 4.

[7] Balakrishnan, J., Dan-Cohen, I., Kim, M., and Wewers, S. (2012). *A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves*. arXiv preprint arXiv:1209.0640.

[8] Berkovich, Vladimir G. *Integration of One-forms on P-adic Analytic Spaces*. (AM-162). No. 162. Princeton University Press, 2007.

[9] Berthelot, Pierre.*Cohomologie Cristalline des Schémas de Caractéristique* $p > 0$ LNM 407, Springer, 1974.

[10] Berthelot, Pierre. *Finitude et pureté cohomologique en cohomologie rigide* https://perso.univ-rennes1.fr/pierre.berthelot/publis/Finitude.pdf

[11] Besser, Amnon. *Coleman integration using the Tannakian formalism*. Mathematische Annalen 322, no. 1 (2002): 19-48.

[12] Besser, Amnon. *Heidelberg lectures on Coleman integration*. In The Arithmetic of Fundamental Groups, pp. 3-52. Springer, Berlin, Heidelberg, 2012.

[13] Besser, Amnon. *Syntomic regulators andp-adic integration I: Rigid syntomic regulators*. Israel Journal of Mathematics 120, no. 2 (2000): 291-334.

[14] Besser, Amnon. *Syntomic regulators and p-adic integration II: K 2 of curves*. Israel Journal of Mathematics 120, no. 2 (2000): 335-359.

[15] Bloch, Spencer. *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves.* Vol. 11. American Mathematical Soc., 2000.

[16] Bochner, S. *Formal Lie Groups*. Annals of Mathematics, vol. 47, no. 2, 1946, pp. 192–201. JSTOR, JSTOR, www.jstor.org/stable/1969242.

[17] Borel, Armand. *Sur La Cohomologie Des Espaces Fibres Principaux Et Des Espaces Homogenes De Groupes De Lie Compacts*. Annals of Mathematics, Second Series, 57, no. 1 (1953): 115-207. doi:10.2307/1969728.

[18] Bostan, Alin, Gaudry, Pierrick, and Schost, Éric. *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator*. SIAM Journal on Computing 36, no. 6 (2007): 1777-1806.

[19] Chen, Kuo-Tsai. *Algebras of iterated path integrals and fundamental groups.* Transactions of the American Mathematical Society 156 (1971): 359-379.

[20] Coleman, Robert F. *Torsion points on curves and p-adic abelian integrals.* Annals of Mathematics 121.1 (1985): 111-168.

[21] Coleman, Robert F. *Effective Chabauty* Duke Math. J 52.3 (1985): 765-770.

[22] Coleman, Robert, and Ehud De Shalit. *p-adic regulators on curves and special values of p-adic L-functions*. Inventiones mathematicae 93, no. 2 (1988): 239-266.

[23] Coleman, Robert F. *Dilogarithms, regulators and p-adic L-functions*. Inventiones mathematicae 69, no. 2 (1982): 171-208.

[24] Coleman, Robert F., and B. Gross. *p-adic Heights on Curves* Math. Sciences Research Inst., Berkeley, Calif. (1987).

[25] Fresnel, Jean, and Marius Van der Put *Rigid analytic geometry and its applications* Vol. 218. Springer Science & Business Media, 2012.

[26] Gabber O, Ramero L. *Almost ring theory*. Springer; 2003 Dec 15.

[27] Gaudry, Pierrick, and Nicolas Gürel. *An extension of Kedlaya's point-counting algorithm to superelliptic curves*. Advances in Cryptology - ASIACRYPT 2001, Springer, Berlin, Heidelberg, 2001.

[28] Gerritzen, L. and Van der Put, M., 2006. *Schottky groups and Mumford curves* (Vol. 817). Springer.

[29] Gonçalves, Cécile. *A point counting algorithm for cyclic covers of the projective line*. Contemporary mathematics 637 (2015): 145.

[30] Goncharov, Alexander. *Mixed elliptic motives*. London Mathematical Society Lecture Note Series (1998): 147-222.

[31] Goncharov, Alexander B., and Andrey M. Levin. *Zagier's conjecture on L (E, 2)*. Inventiones mathematicae 132, no. 2 (1998): 393-432.

[32] Harrison, Michael C. *An extension of Kedlaya's algorithm for hyperelliptic curves*. Journal of Symbolic Computation 47.1 (2012): 89-101.

[33] Hartshorne, Robin. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[34] Harvey, David. *Counting points on hyperelliptic curves in average polynomial time*. Annals of Mathematics 179, no. 2 (2014): 783-803.

[35] Harvey, David. *Kedlaya's Algorithm in Larger Characteristic*. IMRN: International Mathematics Research Notices 2007 (2007).

[36] Harvey, David, and Andrew V. Sutherland. *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*. LMS Journal of Computation and Mathematics 17, no. A (2014): 257-273.

[37] Harvey, David, and Andrew V. Sutherland. *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II*. Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemporary Mathematics 663 (2016): 127-148.

[38] Hida, Haruzo. *Geometric modular forms and elliptic curves*. World Scientific, 2012.

[39] Hulsbergen, Wilfred WJ. *Conjectures in arithmetic algebraic geometry*. Braunschweig: Vieweg, 1992.

[40] Jannsen, Uwe. *Continuous Étale Cohomology*. Mathematische Annalen 280.2 (1988): 207-246.

[41] Katz, Nicholas. *Serre-Tate local moduli*. In Surfaces algébriques, pp. 138-202. Springer, Berlin, Heidelberg, 1981.

[42] Kedlaya, Kiran S. *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. 16 (2001), no. 4, 323-338; errata, ibid. 18 (2003), 417–418.

[43] Lang, Serge, *Algebra*, Graduate Texts in Mathematics 1.211 (2002): ALL-ALL.

[44] Lee, John M. *Smooth manifolds*. Springer, New York, NY, 2003. 9780387954486.

[45] Le Gall, François. *Faster algorithms for rectangular matrix multiplication*. In Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on, pp. 514-523. IEEE, 2012.

[46] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford University Press, 2002.

[47] Matsumura, Hideyuki. *Commutative ring theory*. Vol. 8. Cambridge university press, 1989.

[48] Matsumura, Hideyuki. *Commutative algebra*. Vol. 120. New York: WA Benjamin, 1970.

[49] Mazur, Barry, William Stein, and John Tate. *Computation of p-adic heights and log convergence.* Doc. Math (2006): 577-614.

[50] Mazur, Barry, John Tate, and Jeremy Teitelbaum. *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Inventiones mathematicae 84, no. 1 (1986): 1-48.

[51] Milne, James S. *Etale cohomology* (PMS-33). Vol. 33. Princeton university press, 2016.

[52] Minzlaff, Moritz. *Computing zeta functions of superelliptic curves in larger characteristic*. Mathematics in Computer Science 3.2 (2010): 209-224.

[53] Mumford, David. *Abelian varieties*. Vol. 5. Oxford University Press, USA, 1974.

[54] Narkiewicz, Wladyslaw *Elementary and Analytic Theory of Algebraic Numbers*. Springer, 2004.

[55] Polishchuk, Alexander. *Abelian varieties, theta functions and the Fourier transform*. Vol. 153. Cambridge University Press, 2003.

[56] Rolshausen, Klaus, and Norbert Schappacher. *On the second K-group of an elliptic curve.* Journal für die reine und angewandte Mathematik 495 (1998): 61-77.

[57] *SageMath, the Sage Mathematics Software System (Version 8.1.0)*, The Sage Developers, 2017, http://www.sagemath.org.

[58] Serre, Jean-Pierre. *A course in arithmetic*. Vol. 7. Springer Science & Business Media, 2012.

[59] Serre, Jean-Pierre. *Galois cohomology*. Springer Science & Business Media, 2013.

[60] Serre, Jean-Pierre. *Local algebra*. Springer Science & Business Media, 2000.

[61] Serre, Jean-Pierre, Martin Brown, and Michel Waldschmidt. *Lectures on the Mordell-Weil theorem*. Vol. 2. Braunschweig: Vieweg, 1990.

[62] Shafarevich, Igor R., and Alexey O. Remizov. *Linear algebra and geometry*. Springer Science & Business Media, 2012.

[63] Silverman, Joseph H. *The arithmetic of elliptic curves*. Vol. 106. Springer Science & Business Media, 2009.

[64] Silverman, Joseph H. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Springer Science & Business Media, 2013.

[65] Stacks Project Authors, *The Stacks Project*, https://stacks.math.columbia.edu.

[66] Sutherland, Andrew. *Isogeny volcanoes*. The Open Book Series 1, no. 1 (2013): 507-530. https://msp.org/obs/2013/1-1/obs-v1-n1-p25-s.pdf.

[67] Tamme, Günter. *Introduction to étale cohomology*. Springer Science & Business Media, 2012.

[68] Tuitman, Jan. *Counting points on curves using a map to* $\mathbf{P}^1$. Mathematics of Computation 85.298 (2016): 961-981.

[69] Tuitman, Jan. *Counting points on curves using a map to* $\mathbf{P}^1$*, II*. Finite Fields and Their Applications 45 (2017): 301-322.

[70] van der Geer, G., Moonen, B. *Abelian Varieties*, from https://www.math.ru.nl/~bmoonen/research.html#bookabvar.

[71] Vélu, Jacques. *Isogénies entre courbes elliptiques*. CR Acad. Sci. Paris, Séries A 273 (1971): 305-347.

[72] Voight, John. *Quaternion Algebras*. http://quatalg.org

[73] Waterhouse, William C. *Profinite groups are Galois groups*. Proceedings of the American Mathematical Society 42.2 (1974): 639-640.

[74] Weng, L., and Nakamura, I. *Arithmetic geometry and number theory*, World Scientific, 2006.

[75] Zagier, Don. *The Bloch-Wigner-Ramakrishnan polylogarithm function.* Mathematische Annalen 286, no. 1 (1990): 613-624.

[76] *Pug Template Engine* see pug-lang.com.