Arithmetic on abelian varieties

Pramathanath Sastry

Chennai Mathematical Institute

June 2016 GANITA conference for Kumar Murty

イロト イヨト イヨト イヨト

Definitions

What is an Abelian variety?

This is a report on joint work with V.K. Murty.

- An Abelian variety is an irreducible, smooth projective group variety.
- Elliptic curves (dimension 1),
- Jacobian of a curve of genus g (dimension g).
- In dimension 4 and higher, not every Abelian variety is a Jacobian.
- However, every simple Abelian variety is a quotient of a Jacobian.

・ロト ・日本 ・モート ・モート

Definitions

The dual abelian variety

Fix an abelian variety A over a field k. The dual abelian variety \widehat{A} is the "space" of isomorphism classes of line bundles L on A which are algebraically equivalent to the trivial line bundle \mathcal{O}_A on A in the following sense:

Two line bundles L₀ and L₁ on A are algebraically equivalent if there is a connected variety (or connected algebraic scheme) S over k, two k-rational points s₀ and s₁ of S such, and a line bundle L on A × S such that L|_{A×{s₀}} ≃ L₀ and L|_{A×{s₁}} ≃ L₁.

(Mumford)

A line bundle L on A is algebraically equivalent to \mathcal{O}_A if and only if $t_a^*L \cong L$ for every $a \in A$.

Definitions

Our goal is to realise \widehat{A} as a subvariety of a suitable Grassmannian given *minimal* data about A. E.g. $V = H^0(A, M)$ where M is a very ample line bundle, $V_1 = H^0(A, M \otimes M)$, the natural map $\mu \colon V \otimes_k V \to V_1$ and some important subspaces of V.

Note: We are not given A or M or $M \otimes M$.

- The Grassmannian in which \widehat{A} will be embedded will be a Grassmannian of subspaces of V of a certain fixed dimension.
- Will say more on this later.

Definitions

Hilbert polynomials

Suppose X is a complete k-scheme, L_0 a line bundle on it, and \mathscr{F} a coherent \mathscr{O}_X - module. Then the Grothendieck-Riemann-Roch theorem shows that the expression $\Psi_{\mathscr{F}}(n) (= \Psi_{\mathscr{F}}^{L_0}(n))$ for integers n, given by

$$n\mapsto \chi(X, \mathscr{F}\otimes L_0^n) \qquad (n\in\mathbb{Z})$$

is a polynomial expression in n.

Definition

The polynomial $\Psi_{\mathscr{F}} \in \mathbb{Q}[t]$ is called the *Hilbert polynomial* of \mathscr{F} with respect to L_0 . If Z is a closed subscheme of X, the *Hilbert polynomial of Z* is $\Psi_{\mathscr{O}_Z}$. We will denote it $\Phi_Z(t)$.

イロト イヨト イヨト イヨト

• Have deg $\Psi_{\mathscr{F}} = \dim \operatorname{Supp}(\mathscr{F})$. In particular, if L is a line bundle,

$$\deg \psi_L = \dim X.$$

- If two line bundles (or for that matter closed subschemes) are algebraically equivalent then it is well known that they have the same *Hilbert polynomial* with respect to L₀. The converse is not true – the Quot scheme/Hilbert scheme for a fixed polynomial Ψ need not be connected!
- For us L₀ will be an ample line bundle, in which case Ψ_𝔅(n) can be shown to be a polynomial in n without appealing to GRR (Hilbert showed it — long before Hirzebruch or Grothendieck).

イロン イヨン イヨン イヨン

Riemann-Roch

Fix an abelian variety A of dimension g over a field k.

• (Riemann-Roch for Abelian Varieties) Let L be a line bundle on A and D any divisor such that $\mathscr{O}(D) \cong L$. Then

$$\chi(A, L) = \frac{\int_A D^g}{g!}$$

• So, with D_0 such that $L_0 \cong \mathscr{O}(D_0)$ we have:

$$\Psi_L(n) = \frac{\int_A (D+nD_0)^g}{g!}$$

• In particular (with $\chi_0 := \chi(A, L_0)$):

$$\Psi_{L_0}(t)=(1+t)^g\chi_0.$$

イロト イポト イヨト イヨト

Algebraically trivial bundles

As we pointed out, if $L \sim_{alg} L'$, then $\Psi_L = \Psi_{L'}$, but that the converse is not in general true. There are important situations (which we exploit) where this is true. First, for a line bundle L let $K(L) = \{a \in L \mid t_a^*L \cong L\}$.

Proposition

Let *L* be a line bundle on *A*, and $d = \dim K(L)$. Then (a) (Moonen-Van der Geer) $\Psi_L(t) = t^d f(t)$, $f(0) \neq 0$, $f \in \mathbb{Q}[t]$. (b) $L \sim_{\text{alg}} \mathscr{O}_A \iff \Psi_L(t) = \chi_0 t^g \iff \Psi_L(t) = ct^g$, with *c* a constant.

In particular, algebraic equivalence with the trivial bundle is completely characterised by the Hilbert polynomial.

・ロン ・回 と ・ 回 と ・ 回 と

2

Ample bundles

Hilbert polynomials also let us figure our when line bundles are ample on and abelian variety.

Theorem (Mumford-Kempf-Ramanujam)*

(a) L is ample if and only if all its complex roots are negative real numbers.

(b) L ample
$$\implies \Psi_L(n) = \mathrm{H}^0(A, L \otimes L_0^n), n \ge 0.$$

Corollary to the last two theorems

$$L \sim_{\mathsf{alg}} L_0 \iff \Psi_L(t) = \chi_0(1+t)^g.$$

イロト イポト イラト イラト

- L a line bundle on $A \Longrightarrow \Psi_{L^{-1}}(t) = (-1)^g \Psi_L(t)$ (Use the identity $(-D + nD_0)^g = (-1)^g (D - nD_0)^g$ and GRR.)
- Suppose $L_0 = \mathscr{O}_A(H)$, where H is effective. The exact sequence

$$0 \longrightarrow \mathscr{O}(-H) \longrightarrow \mathscr{O}_A \longrightarrow \mathscr{O}_H \longrightarrow 0$$

gives us the formula for $\Phi_H(t)$ (the Hilbert polynomial of H)

$$\Phi_H(t) = \chi_0[t^g - (t-1)^g].$$

 In particular, all effective divisors algebraically equivalent to H have Hilbert polynomial

$$\Phi(t):=\chi_0[t^g-(t-1)^g].$$

イロン イヨン イヨン イヨン

The embedding

- Fix $N \ge 2$ and set $V = H^0(A, \mathcal{O}(NH))$.
- For $D \ge 0$ and $D \sim_{\mathsf{alg}} H$, let

 $W_D := \mathrm{H}^0(\mathscr{O}(NH - D)) \subset V.$

- Have $NH D \sim_{alg} (N 1)H$. Hence - NH - D is ample.
 - dim $W_D = \chi_0 (N-1)^g = r$ (say).
- For $N \ge 3g + 2$, the map $D \mapsto W_D$ gives an embedding

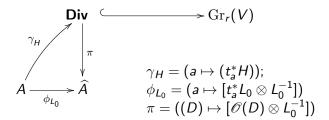
$$\mathsf{Div} \hookrightarrow \mathrm{Gr}_r(V),$$

where

-
$$\operatorname{Div}(=\operatorname{Div}^{L_0}) = \{D \ge 0 \mid D \sim_{\operatorname{alg}} H\}.$$

- $\operatorname{Gr}_r(V)$ = Grassmannian of *r*-dimensional subspaces of *V*

The Grothendieck-Matsusaka method



(a)(Mumford) The map ϕ_{L_0} is an *isogeny*. (b) The map π is surjective, and the fibre of π over [L] is the complete linear system associated with the ample bundle $L \otimes L_0$. (c) If L_0 is a *principal polarisation*, i.e., dim $\mathrm{H}^0(A, L_0) = 1$, then all arrows in the above diagram are isomorphisms.

Let $N \ge 3$ and $V = H^0(A, L_0^N) = H^0(A, \mathcal{O}(NH))$. For each effective divisor D we have associated a subspace $W_D = H^0(\mathcal{O}(NH - D)) \subset V$. One can go the other way.

Definition

Suppose $0 \neq W \subset V$ is a *k*-vector space. Let ϑ be the complete linear system associated with L_0^N and $\vartheta_W \subset \vartheta$ the sub-linear system given by W. Define Δ_W to be the fixed component of ϑ_W .

Note that for a prime divisor Z in A,

$$\operatorname{ord}_{Z} \Delta_{Q} = \min_{s \in W \smallsetminus \{0\}} \left\{ \operatorname{ord}_{Z}(s) + \operatorname{ord}_{Z}(NH) \right\}.$$



Definition

For $D \ge 0$, let

$$D^* := \Delta_{W_D}$$

Would like D to equal D^* . The exact relationship is

Proposition

Let $D \ge 0$ and F the fixed component of the complete linear system defined by $\mathscr{O}(NH - D) = L_0^N \otimes \mathscr{O}(-D)$. Then

$$D^* = D + F.$$

In particular $D^* \ge D$, and $D^* = D$ if and only if the complete linear system |NH - D| has no fixed components.

イロン イヨン イヨン イヨン

In this slide, D, D' etc are effective divisors.

•
$$W_{D^*} = W_D$$
.

•
$$D \leq D' \implies W_D \supset W_{D'}$$
.

• Suppose |NH - D'| has no fixed components. Then $W_D \supset W_{D'} \implies D \le D'$.

・ロン ・回 と ・ヨン ・ヨン

The flip operation

When is $W = W_D$ for some $D \ge 0$? The answer involves the *flip* operation.

Definition

Suppose W is a non-zero subspace of V and $0 \neq f \in W$. Define a subspace W' (= W'(f)) by the formula

$$W' = \{s \in V \mid \mu(s \otimes t) \in \mu(f \otimes V), t \in W\}.$$

• Note: $f \in W'$, and so it makes sense to compute W'' = (W'(f))'(f).

Fact

$$W = U', \ U \neq 0 \implies W = W_D$$
 for some $D \ge 0$.

More precisely, we have (all "flips" with respect to f as in the statement):

Let W be a subspace of V, $0 \neq f \in W$, of V and E the effective divisor $NH - \Delta_W + (f)$.

- Turns out, $W' = W_E$.
- In particular, if W = W'', then $W = W_D$ for some $D \ge 0$.
- The condition W = W'' can be tested using linear algebra.

イロト イポト イヨト イヨト

Absolutely simple abelian varieties

Suppose A is absolutely simple, L a line bundle on A, D a divisor on A.

- Either $L \sim_{alg} \mathscr{O}_A$ or L is *non-degenerate*, i.e., K(L) is finite.
- L ample $\iff L \ncong \mathscr{O}_A$ and $\mathrm{H}^0(A, L) \neq 0$.
- D ample $\iff D \equiv D'$, D' > 0.
- h⁰(L) > 1 ⇒ the complete linear system given by L has no fixed components.

イロン イヨン イヨン イヨン

Assumptions and strategy

Recall we are trying to look for the locus of **Div** in a Grassmanian of subspaces of $V = H^0(L_0^N)$. From now on we will assume

- A is absolutely simple of dimension g and as before
- L_0 is a principal polarization, i.e., $H^0(L_0) = 1$.

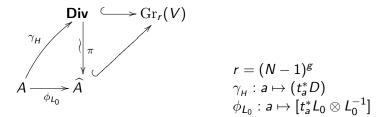
Preliminary Strategy

Let a non-zero subspace W of V be given. Pick $0 \neq f \in W$.

- Check if W = W''. So we know $W = W_D$ for some $D \ge 0$.
- For j = 0, ..., g find a subspace $T_j(W)$ by linear algebraic means so that $T_j(W) = W_{D+jH}$.
- Check that dim $T_j(W) = \chi_0(N-j-1)^g = (-1)^g \Psi(j-N)$. This will force $\Psi_{\mathscr{O}(D)}(t)$ to equal $\Psi(t) = \chi_0(1+t)^g$.



 $D_j = D + jH$



イロン イヨン イヨン イヨン

Forward and backward shifts

Goal: Given $0 \neq W \subset V$, define $T_j(W) \subset W$. $(T_j(W_D)^{"} = "W_{D+jH})$. Fix $j \geq 0$. Assume we know the canonical map $\mu: V \otimes_k V \to H^0(A, L_0^{2N})$, and the spaces $H^0(L_0^j)$ and $H^0(L_0^{N-j})$. (We only need j = 3, 4, 5).

- $T_j(W) := \{ s \in W \mid \mu(s \otimes t) \in \mu(W \otimes_k \mathrm{H}^0(L_0^{N-j})), \forall t \in V \}.$
- $\mu_j(W) := \mu(W \otimes_k \mathrm{H}^0(L_0^j)) \subset \mathrm{H}^0(L_0^{2N}). \ (\mu_j(W_D)^{"} = "W_{D-jH})$
- $T_j(W_D) \subset W_{D+jH}$
- $\mu_j(W_D) \subset W_{D-jH}$ provided D jH is effective.

イロン イ部ン イヨン イヨン 三日

m-regularity

- A coherent sheaf on a projective scheme (X, 𝒪(1)) is *m*-regular if Hⁱ(X, 𝓕(m-i)) = 0 for i ≥ 1.
- (Mumford) If \mathscr{F} is *m*-regular then it is (m + 1)-regular and the natural map $\mathrm{H}^{0}(\mathscr{F}(m)) \otimes_{k} \mathrm{H}^{0}(\mathscr{O}(1)) \to \mathrm{H}^{0}(\mathscr{F}(m+1))$ is surjective.
- Returning to our abelian variety A, if L is ample then L is g-regular $(g = \dim A)$. Indeed, we only have to check

$$\mathrm{H}^{i}(A, L(g-i)) = 0 \qquad (\text{for } 0 < i \leq g).$$

In that range $g - i \ge 0$, whence $L \otimes \mathscr{O}(g - i)$ is ample.

We did not need absolute simplicity of A for the above, but if it is (our running assumption), then h⁰(L) > 1 ensures ampleness of L.

• Let
$$D, D' \ge 0$$
 with dim $W_D > 1$. Fix $j \in \{1, ..., N-3\}$. Then
 $T_j(W_{D'}) = W_D$ and $\mu_j(W_D) = W_{D'} \Longrightarrow D = D' + jH$.

• Let $3 \leq j < \frac{N}{g+1}$. Suppose D is an effective divisor such that $L_0^{N-j} \otimes \mathscr{O}(-D)$ is 0-regular with respect to L_0^j . Then

$$T_j(W_D) = W_{D+jH}$$
 and $\mu_j(W_{D+jH}) = W_D$.

- The above is (of course) for A absolutely simple.
- Recall also that if W = W'', then $W = W_D$ for some $D \ge 0$.
- $L_0^{N-j} \otimes \mathscr{O}(-D)$ is 0-regular $\iff L_0^{N-j-g} \otimes \mathscr{O}(-D)$ is g-regular. A sufficient condition is that $h^0(L_0^{N-j-g} \otimes \mathscr{O}(-D)) > 1$. This is ensured when $T^{j+g}(W_D) > 1$.

イロン イヨン イヨン イヨン

From now on

- N = 6g + 6, $r = (6g + 5)^g$.
- $V = H^0(A, L_0^N)$.

Assumptions

Assume we know

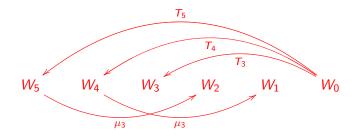
- $\mu \colon V \otimes_k V = \mathrm{H}^0(L_0^N) \otimes_k \mathrm{H}^0(L_0^N) \to \mathrm{H}^0(L_0^{2N}),$
- $H^0(L_0^j)$ and $H^0(L_0^{N-j})$ for j = 3, 4, 5.

Consider the embedding:

$$\operatorname{Gr}_r(V) \hookrightarrow \mathsf{Div}$$

Given a subspace $W \subset V$ of dimension r, i.e., a point $x_w \in \operatorname{Gr}_r(V)$, how does one decide whether $x_w \in \operatorname{Div} or$ not?

Let $W_0 = W$. Get W_1 , W_2 , W_3 , W_4 and W_5 as follows:

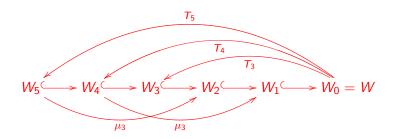


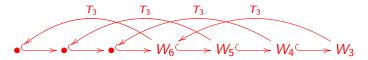
Define W_g , W_{g-1} , ..., W_6 , via the formula

$$W_{i+3} = T_3(W_i)$$
 $(i = 3, ..., g - 3).$

・ロト ・回ト ・ヨト ・ヨト

Impose the following conditions:





< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

Let W be an r-dimensional subspace of V and x_W the corresponding point in $\operatorname{Gr}_r(V)$. Then $x_W \in \operatorname{Div}$ if and only if W satisfies conditions (1)—(7) above.

イロン イヨン イヨン イヨン

Thank you!

Pramathanath Sastry Arithmetic on abelian varieties

・ロン ・四 と ・ ヨ と ・ モ と

Addition

Let F = μ(T₃^{g+1}(W¹) ⊗_k T₃^{g+1}(W²)). One can show:
F ⊂ V. (If W¹ = W_D, and W² = W_E, then F = W_{D+E}.)
dim F = (N - 2)^g = (6g + 4)^g.
0 ≠ μ₃(T₅(F)) ⊂ F.
Pick 0 ≠ φ ∈ μ₃(T₅(F)). Use φ to compute F', i.e., F' = F'(φ). Note that φ ∈ F', whence F' ≠ 0.
Pick 0 ≠ ψ ∈ F' such that

$$\mu(\psi \otimes \mathrm{H}^{0}(\mathscr{O}(3H))) \subset (\mu_{3}T_{5}F)'.$$

One can show that such a ψ exists and is unique up to a non-zero scalar multiple.

・ロン ・回 と ・ 回 と ・ 回 と

• Let
$$U = \{s \in V \mid \mu(\varphi \otimes s) \in \mu(\psi \otimes F)\}$$
. (Theory shows that $U \subset V$.)

Set $W = \mu_4(T_3(U))$. Then $W = W^1 * W^2$. In other words

$$x_W = x_{W_1} + x_{W_2}.$$

・ロン ・回 と ・ ヨ と ・ ヨ と

3