Generalizations of Deuring's Mass Formula

Gerard van der Geer

This is a short version of the talk given at San-Feliu-de-Guixols on October 29, 1997. In the talk I discussed joint work with Torsten Ekedahl. A preliminary version of this work can be found in the preprint `alg-geom 9605011`.

1. Deuring's Formula

On an elliptic curve E over an algebraically closed field k multiplication by n defines a morphism of degree n^2. If $p = char(k)$ does not divide n, then $\times n$ is étale and the kernel satisfies $\#E[n](k) = n^2$. However, $\times p$ is inseparable and $\#E[p](k) = p$ if E is ordinary and $\#E[p](k) = 1$ if E is *supersingular*. Hasse proved in 1934 that there is a polynomial A such that E is supersingular if and only if $j(E)$ is a root of A. In 1941 Deuring showed that if E is supersingular then $\mathrm{End}(E) \otimes \mathbb{Q} \cong D_{\infty,p}$, the quaternion division algebra ramified at p and ∞, and the number of such E is the class number h of $D_{\infty,p}$. Combination with a formula of Eichler for this class number h gives:

Deuring's Mass Formula. *We have*

$$\sum_{[E]} \frac{1}{\#\mathrm{Aut}(E)} = \frac{p-1}{24},$$

where the sum is over the isomorphism classes $[E]$ of supersingular elliptic curves $/k$.

For example, for $p = 2$ the only curve is $y^2 + y = x^3$ with $\#\mathrm{Aut}(E) = 24$. If one uses the Legendre form of an elliptic curve $y^2 = x(x-1)(x-\lambda)$ Hasse's polynomial A for $p \geq 3$ is:

$$A = (-1)^{(p-1)/2} \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 \lambda^i.$$

2. Abelian Varieties

We shall generalize the formula of Deuring. The notion of elliptic curve is replaced by the notion of principally polarized abelian variety, i.e. an abelian variety X together with $\lambda : X \xrightarrow{\sim} \hat{X} = \mathrm{Pic}^0(X)$. If X is a principally polarized abelian variety of dimension g the kernel $X[p] := \ker(\times p)$ is a group scheme of order p^{2g}. If k is of characteristic $p > 0$ we have the *Frobenius* map $F : X \to X^{(p)}$, $\mathrm{coord}(x) \mapsto \mathrm{coord}(x)^p$, where $X^{(p)}$ is obtained from X by raising the coefficients in the equations of X to the p-th power. This F induces a dual map (*Verschiebung*)

$$V : X^{(p)} \cong \hat{X}^{(p)} \to \hat{X} \cong X.$$

satisfying $V \cdot F = p_X$ and $F \cdot V = p_{X^{(p)}}$. In the case of elliptic curves inseparability of V implies $\ker(V) = \ker(F^{(p)})$, the unique connected subgroup scheme of rank p.

`san-feliu-abstract`

3. The Moduli Space

The j-line generalizes to $\mathcal{A}_g$, the moduli space of principally polarized abelian varieties of dimension g. It is a stack (or orbifold) of dimension is $g(g+1)/2$. Over $\mathbb{C}$ we have

$$\mathcal{A}_g(\mathbb{C}) = H_g/Sp(2g,\mathbb{Z}).$$

We sometimes need a good compactification $\tilde{\mathcal{A}}_g$, a Faltings-Chai compactification. The stack $\mathcal{A}_g$ carries a "universal abelian variety" $\mathcal{X}_g \to \mathcal{A}_g$. The cotangent bundle at the 0-section s of $\mathcal{X}_g$ defines a vector bundle (*the Hodge bundle*)

$$\mathbb{E} := s^*(\Omega^1_{\mathcal{X}})$$

of rank g over $\mathcal{A}_g$ (and $\tilde{\mathcal{A}}_g$). We define tautological classes $\lambda_i(\mathbb{E}) = c_i(\mathbb{E}) \in CH^i_{\mathbb{Q}}(\mathcal{A}_g)$, the i-th Chern class (in the Chow ring $CH_{\mathbb{Q}}$ or in the cohomology). These generate a subring called the 'tautological subring'.

Theorem. *These λ_i satisfy the relations*

$$(1+\lambda_1+\ldots+\lambda_g)(1-\lambda_1+\ldots+(-1)^g\lambda_g) = 1.$$

Moreover,

$$\lambda_g = 0 \quad \text{on } \mathcal{A}_g \text{ (but not on } \tilde{\mathcal{A}}_g\text{)}$$

Both follow from applying Grothendieck-Riemann-Roch. There are no further relations. We can calculate the tautological Chern numbers for our compactication $\tilde{\mathcal{A}}_g$:

The Proportionality Principle of Hirzebruch and Mumford. *The ratio between top degree polynomials in the λ_i is the same as for the compact dual of the Siegel upper half space H_g.*

Using the Euler number (due to Siegel and Harder) we find:

$$\lambda_1\lambda_2\ldots\lambda_g[\tilde{\mathcal{A}}_g] = (-1)^{g(g+1)/2}\prod_{j=1}^{g}\frac{\zeta(1-2j)}{2}.$$

Examples:

$$\begin{aligned} g&=1 \qquad \deg(\lambda_1) = 1/24,\\ g&=2 \qquad \deg(\lambda_1^3) = 1/2880,\\ g&=3 \qquad \deg(\lambda_1^6) = 1/181440. \end{aligned}$$

4. A stratification

We generalize the notion of supersingularity by looking at the operators F and V. Instead of $X[p]$ consider $H = H^1_{dR}(X)$, a vector space of dimension $2g$. It comes with two operators: V which is σ^{-1}-linear and F which is σ-linear. On it we have a non-degenerate pairing $\langle\ ,\ \rangle$ and V and F are adjoint $\langle Vh, h'\rangle = \langle h, Fh'\rangle$. The spaces $V(H) = F^{-1}(0)$ and $F(H) = V^{-1}(0)$ are maximal isotropic. We consider (symplectic) filtrations

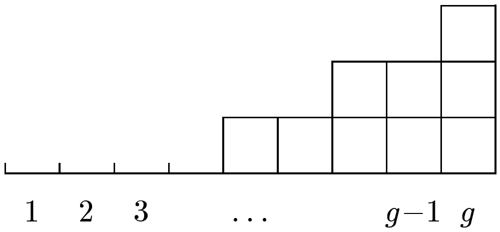
$$0 \subset E_1 \subset \ldots \subset E_g \subset E_{g+1} \subset \ldots \subset E_{2g} = H$$

with $V(E_{2g}) = E_g$, $E_{g-i}^{\perp} = E_{g+i}$, and $\dim(E_i) = i$. Such a filtration is not unique, but its "type" ν is:

$$\nu : \{0, 1, 2, \ldots, 2g\} \to \{0, 1, 2, \ldots, g\}$$

with $\nu(2g - i) = \nu(i) - i + g$ for $0 \leq i \leq g$. It is defined by $V(E_i) = E_{\nu(i)}$. We can make a stratification of $\mathcal{A}_g$ by types. This is the Ekedahl-Oort-stratification. (They introduced it in a slightly different way.)

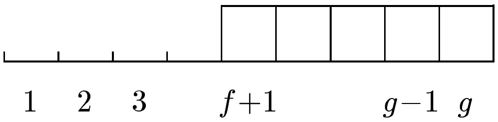
We can visualize the conditions by the associated Young-type diagram with μ_j squares in the j-th layer by putting a stack of $i - \nu(i)$ squares in position i: e.g. for $\mu = \{5, 3, 1\}$:



The meaning of this is: the height at place i equals $= \dim \ker V|E_i$. Note that there are 2^g such diagrams.

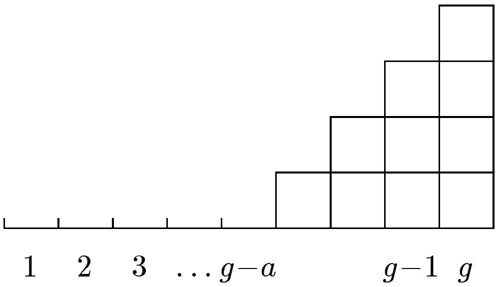
Examples.

- $g = 1$: 2 possibilities $\emptyset$ and $\square$ (ordinary and supersingular)
- p-rank $\leq f$:



corresponding locus $\quad V_f = \{[X] \in \mathcal{A}_g : \#X[p](k) \leq p^f\}$

- a-number $\geq a$;



corresponding locus $\quad T_a = \{[X] \in \mathcal{A}_g : \dim \mathrm{Hom}(\alpha_p, X) \geq a\}$

To define loci in general, consider

$$0 \to H^0(\Omega^1) \to H^1_{dR}(X) \to H^1(O_X) \to 0,$$

or over the whole moduli space $0 \to \mathbb{E} \to \mathbb{H} \to \mathbb{E}^{\perp} \to 0$. We have two symplectic filtrations on the Hodge bundle: $\mathbb{E}_i$ $(i = 1, \ldots, g)$, the given one. We make a second one, starting from $\mathbb{F}_g = \ker(V) = V^{-1}(0)$, and setting

$$\mathbb{F}_{g+i} = V^{-1}(\mathbb{E}_i^{(p)}), \qquad \mathbb{F}_{g-i} = \mathbb{F}_{g+i}^{\perp}.$$

We shall compare the two filtrations. Consider the space $\mathcal{F} = \mathrm{Flag}(\mathbb{H})$ of symplectic flags. This space has dimension g^2 and lives over $\mathcal{A}_g$ via the canonical map $\mathcal{F} \to \mathcal{A}_g$. Define for a diagram μ a locus $\mathcal{U}_\mu \subset \mathcal{F}$ by: $\ker(V) \cap \mathbb{E}_i \geq$ height of the diagram in position i, or more precisely, the locus of all flags with $V(\mathbb{E}_i) \subseteq \mathbb{E}_{\nu(i)}$.

5. The Classes

We start with the simplest case: $\mu = \emptyset$. The locus $\mathcal{U}_\emptyset$ has codimension $g(g-1)/2$ in $\mathcal{F}$. It is a finite cover of $\mathcal{A}_g$ and can be viewed as a component of "$\Gamma_0(p)$". The degree of the cover is $(p+1)(p^2+p+1)\ldots(p^g+p^{g-1}+\ldots+1)$.

The next interesting case is the locus V_f of X with p-rank $\leq f$. By Oort we know that its codimension in $\mathcal{A}_g$ or $\mathcal{U}_\emptyset$ is $g-f$. We can calculate the class of V_f in the Chow ring of $\mathcal{U}_\emptyset$. If $\pi : \mathcal{U}_\emptyset \to \mathcal{A}_g$ then we can show in $CH_{\mathbb{Q}}(\mathcal{U}_\emptyset)$:

$$[\pi^{-1}(V_f)] = (p-1)^{g-f}\lambda_{g-f}.$$

Theorem. *On $\tilde{\mathcal{A}}_g$ the class of the p-rank $\leq f$ locus V_f is given by*

$$[V_f] = (p-1)(p^2-1)\ldots(p^{g-f}-1)\lambda_{g-f}.$$

The simplest example is $g=1$, $f=0$. We have $[V_0] = (p-1)\lambda_1$. But $\deg(\lambda_1) = 1/24$, so $\deg([V_0]) = (p-1)/24$, which is exactly Deuring's formula. So these formulas are generalizations of Deuring's formula. An interesting by-product is that they also show that the λ_i can be represented by *effective* cycles.

Another case is the locus of a-number $\geq a$:

$$T_a = \{[X] \in \mathcal{A}_g : \mathrm{rank}(V)|\mathbb{E}_g \leq g-a\} = \{[X] \in \mathcal{A}_g : \dim \mathrm{Hom}(\alpha_p, X) \geq a\}.$$

Define for a symplectic bundle A with Chern classes a_i the expression

$$Q_{ij} := a_i a_j + 2\sum_{k=1}^{j} a_{i+k}a_{j-k} \qquad (i > j)$$

For a partition $\beta = (\beta_1, \ldots, \beta_r)$ with r even set $Q_\beta = \mathrm{Pfaffian}(Q_{\beta_i\beta_j})$. Using degeneracy formulas of Pragacz and Ratajski we can prove:

Theorem. *The class of the a-number $\geq a$ locus T_a of is given by the formula*

$$[T_a] = \sum_\beta Q_\beta(\mathbb{E}^{(p)})Q_{\rho(a)-\beta}(\mathbb{E}^*),$$

where the sum is over all admissible diagrams β contained in $\rho(a) = (a, a-1, \ldots, 1)$.

Examples

$$\begin{aligned}
[T_1] &= (p-1)\lambda_1 \\
[T_2] &= (p-1)(p^2+1)\lambda_1\lambda_2 - (p^3-1)\lambda_3 \\
&\vdots \\
[T_g] &= (p-1)(p^2+1)\ldots(p^g+(-1)^g)\,\lambda_1\lambda_2\ldots\lambda_g
\end{aligned}$$

The most degenerate case is T_g which consists of finitely many points. Writing out the meaning of the formula gives:

$$\sum_{X, a(X)=g} \frac{1}{\#\mathrm{Aut}(X)} = \pm \prod_{j=1}^{g} \frac{(p^j + (-1)^j)\zeta(1-2j)}{2}.$$

Using formulas for symplectic degeneray loci of Fulton we get an expression for the class of $\mathcal{U}_\mu$ in $\mathcal{U}_\emptyset$. It is a complicated polynomial in p and the ℓ_i. We can calculate the push forward to $\mathcal{A}_g$ algorithmically. The class of the push forward in $CH^*_{\mathbb{Q}}(\tilde{\mathcal{A}}_g)$ is a polynomial in p and the λ_i.

The penultimate stratum $\mu = (g, g-1, \ldots, 2)$ is a configuration of $\mathbb{P}^1$'s in $\mathcal{A}_g \otimes \mathbb{F}_p$. This contrasts with the characteristic 0 case, where $\mathcal{A}_g(\mathbb{C})$ does not contain lines.

We can prove irreducibility for certain loci:

Theorem. *The locus T_a for $a < g$ is irreducible.*

For $g = 1$ and $g = 2$ the *supersingular locus* is a stratum from the Ekedahl-Oort stratification. But for higher g it is not. The definition of this stratum involves not only $X[p]$, but the higher $X[p^n]$ as well. We can calculate it for $g = 3$:

Theorem. *The class of the supersingular locus in $\mathcal{A}_3$ is*

$$[S_3] = (p-1)(p^2-1)(p^3-1)(p-1)(p^2+1)\lambda_1\lambda_3.$$

We do not know for higher g whether these classes $[S_g]$ lie in the tautological ring.

For more details we refer the interested reader to:

G. van der Geer: Cycles on the moduli space of abelian varieties. Preprint. `alg-geom 9605011`

Gerard van der Geer
Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
Nederland
e-mail: `geer@wins.uva.nl`