The p-kernel of abelian varieties in characteristic p

Milan Lopuhaä-Zwakenberg[1]

[1]Institute of Mathematics, Astrophysics and Particle Physics
Radboud University, Nijmegen, the Netherlands

Young Researchers in Mathematics 2017

Affine algebraic groups

Let k be a field. All k-algebras are commutative and unital.

Definition

A *affine algebraic group over k* is a quadruple $G = (A, \Delta, \eta, \iota)$ consisting of

- a k-algebra A;
- a morphism $\Delta\colon A \to A \otimes_k A$ 'comultiplication',
- a morphism $\eta\colon A \to k$ 'counit',
- a morphism $\iota\colon A \to A$ 'coinversion',

satisfying 'some axioms'.

Affine algebraic groups

If $G = (A, \Delta, \eta, \iota)$ is an affine algebraic group, and R is a k-algebra, set $G(R) := \mathrm{Hom}(A, R)$. Then we get:

- A binary operator 'multiplication'
  $G(R) \times G(R) \cong \mathrm{Hom}(A \otimes A, R) \xrightarrow{\Delta^*} \mathrm{Hom}(A, R) = G(R)$;

Affine algebraic groups

If $G = (A, \Delta, \eta, \iota)$ is an affine algebraic group, and R is a k-algebra, set $G(R) := \mathrm{Hom}(A, R)$. Then we get:

- A binary operator 'multiplication'
  $G(R) \times G(R) \cong \mathrm{Hom}(A \otimes A, R) \xrightarrow{\Delta^*} \mathrm{Hom}(A, R) = G(R)$;
- A distinguished 'unit element' $1 \in G(R)$ given by the composition
  $A \xrightarrow{\eta} k \to R$;

Affine algebraic groups

If $G = (A, \Delta, \eta, \iota)$ is an affine algebraic group, and R is a k-algebra, set $G(R) := \mathrm{Hom}(A, R)$. Then we get:

- A binary operator 'multiplication'
  $G(R) \times G(R) \cong \mathrm{Hom}(A \otimes A, R) \xrightarrow{\Delta^*} \mathrm{Hom}(A, R) = G(R)$;
- A distinguished 'unit element' $1 \in G(R)$ given by the composition $A \xrightarrow{\eta} k \to R$;
- A map 'inversion' $G(R) \to G(R)$ given by $\mathrm{Hom}(A, R) \xrightarrow{\iota^*} \mathrm{Hom}(A, R)$.

Affine algebraic groups

If $G = (A, \Delta, \eta, \iota)$ is an affine algebraic group, and R is a k-algebra, set $G(R) := \mathrm{Hom}(A, R)$. Then we get:

- A binary operator 'multiplication' $G(R) \times G(R) \cong \mathrm{Hom}(A \otimes A, R) \xrightarrow{\Delta^*} \mathrm{Hom}(A, R) = G(R)$;
- A distinguished 'unit element' $1 \in G(R)$ given by the composition $A \xrightarrow{\eta} k \to R$;
- A map 'inversion' $G(R) \to G(R)$ given by $\mathrm{Hom}(A, R) \xrightarrow{\iota^*} \mathrm{Hom}(A, R)$.

For a right choice of 'some axioms' this turns $G(R)$ into a group.

Definition

The *order* of G is $\dim_k(A)$.

Examples

Γ abstract group: take

- $A = \bigoplus_{\gamma \in \Gamma} k \cdot e_\gamma$;
- $\Delta(e_\gamma) = \sum_{\gamma'\gamma''=\gamma} e_{\gamma'} \otimes e_{\gamma''}$;
- $\eta =$ projection onto $k \cdot e_1 \cong k$;
- $\iota(e_\gamma) = e_{\gamma^{-1}}$.

Then $G(k') = \Gamma$ for every field ext. k'/k, and the order of G is $\#\Gamma$.

Examples

- take $A = k[X]$, then $G(R) = R$: additive group $\mathbb{G}_{\mathsf{a}}$.

Examples

- take $A = k[X]$, then $G(R) = R$: additive group $\mathbb{G}_{\mathsf{a}}$.
- take $A = k[X, Y]/(XY - 1)$, then $G(R) = R^{\times}$: multiplicative group $\mathbb{G}_{\mathsf{m}}$.

Examples

- take $A = k[X]$, then $G(R) = R$: additive group $\mathbb{G}_{\mathsf{a}}$.
- take $A = k[X, Y]/(XY - 1)$, then $G(R) = R^{\times}$: multiplicative group $\mathbb{G}_{\mathsf{m}}$.
- take $A = k[X]/(X^n - 1)$, then $G(R) = \{r \in R : r^n = 1\}$: nth roots of unity μ_n.

In the last example, $\mathrm{ord}(\mu_n) = n$, but in general $\#\mu_n(k) \leq n$.

Abelian varieties

Definition

An *abelian variety* over k is a connected smooth projective group variety over k.

Abelian varieties

Definition

An *abelian variety* over k is a connected smooth projective group variety over k.

Proposition

The group structure on an abelian variety is commutative.

Abelian varieties

Definition

An *abelian variety* over k is a connected smooth projective group variety over k.

Proposition

The group structure on an abelian variety is commutative.

Proposition

If A is an abelian variety of dimension g, then its p-kernel $A[p]$ is a commutative affine algebraic group of order p^{2g} and exponent p.

Question: Can we classify all possible $A[p]$?

Classifying $A[p]$

Suppose $k = \bar{k}$.

- If $\mathrm{char}(k) \neq p$, then only one group scheme of order p^{2g} and exponent p: the group scheme corresponding to $(\mathbb{Z}/p\mathbb{Z})^{2g}$.

Classifying $A[p]$

Suppose $k = \bar{k}$.

- If $\mathrm{char}(k) \neq p$, then only one group scheme of order p^{2g} and exponent p: the group scheme corresponding to $(\mathbb{Z}/p\mathbb{Z})^{2g}$.
- If $\mathrm{char}(k) = p$ more possibilities: consider μ_p.
  - $\mu_p(k) = 1$
  - take $R = k[\varepsilon]/(\epsilon^2)$; then $\mu_p(R) = 1 + k\varepsilon$.

Dieudonné theory

A commutative group scheme of order p^n and exponent p over k corresponds to a *Dieudonné module of dimension* g, i.e. a triple (D, F, V) consisting of

- A k-vector space D of dimension g;
- Two additive maps $F, V\colon D \to D$ such that for all $\lambda \in k^\times$

$$FV = VF = 0, F\lambda = \lambda^p F, V\lambda^p = \lambda V.$$

Dieudonné theory

A commutative group scheme of order p^n and exponent p over k corresponds to a *Dieudonné module of dimension* g, i.e. a triple (D, F, V) consisting of

- A k-vector space D of dimension g;
- Two additive maps $F, V\colon D \to D$ such that for all $\lambda \in k^\times$

$$FV = VF = 0, F\lambda = \lambda^p F, V\lambda^p = \lambda V.$$

Proposition

If (D, F, V) corresponds to $A[p]$ for some abelian variety A, then $\mathrm{im}(F) = \ker(V)$ *(hence* $\mathrm{im}(V) = \ker(F)$*).*

Classifying Dieudonné modules

So next two questions:

1. Can we classify Dieudonné modules of dimension n over k with $\mathrm{im}(F) = \ker(V)$?
2. Which of these correspond to $A[p]$ for some A?

For the remainder of this talk we focus on the first question.

The stack D_n

For a $\mathbb{F}_p$-algebra R, set $\mathsf{D}_n(R) :=$ category of Dieudonné modules of dimension n over R. Then

$$\mathsf{D}_n \colon \mathsf{Alg}_{\mathbb{F}_p} \to \mathsf{Cat}$$

is a *stack* $\approx$ categorical construction with some 'geometric structure'.

The stack D_n

For a $\mathbb{F}_p$-algebra R, set $\mathsf{D}_n(R) :=$ category of Dieudonné modules of dimension n over R. Then

$$\mathsf{D}_n \colon \mathsf{Alg}_{\mathbb{F}_p} \to \mathsf{Cat}$$

is a *stack* $\approx$ categorical construction with some 'geometric structure'. We can count the 'points' of D_g by means of the zeta function:

$$Z(\mathsf{D}_n, t) = \exp\left(\sum_{v \geq 1} \frac{t^v}{v} \sum_{D \in [\mathsf{D}_n(\mathbb{F}_{p^v})]} \frac{1}{\#\mathsf{Aut}(D)}\right) \in \mathbb{Q}[[t]]$$

with $[\mathsf{D}_n(\mathbb{F}_{p^v})] := \mathsf{Ob}(\mathsf{D}_n(\mathbb{F}_{p^v}))/\cong$.

Main result (for now)

Theorem

There exist a finite set $\mathcal{I}$ and a function $d\colon \mathcal{I} \to \mathbb{Z}_{\geq 0}$ that can explicitely be described, such that

$$Z(D_n, t) = \prod_{i \in \mathcal{I}} \frac{1}{1 - p^{d(i)} t}.$$

Next: sketch of how to obtain this result.

Canonical filtration

Let $D \in \mathrm{D}_n(k)$. Then the *canonical filtration* on D is the coarsest filtration $0 = D_0 \subset D_1 \subset \ldots \subset D_r = D$ such that for every i, $F(D_i) = D_j$ and $V^{-1}(D_i) = D_{j'}$ for some $j, j' \leq n$.

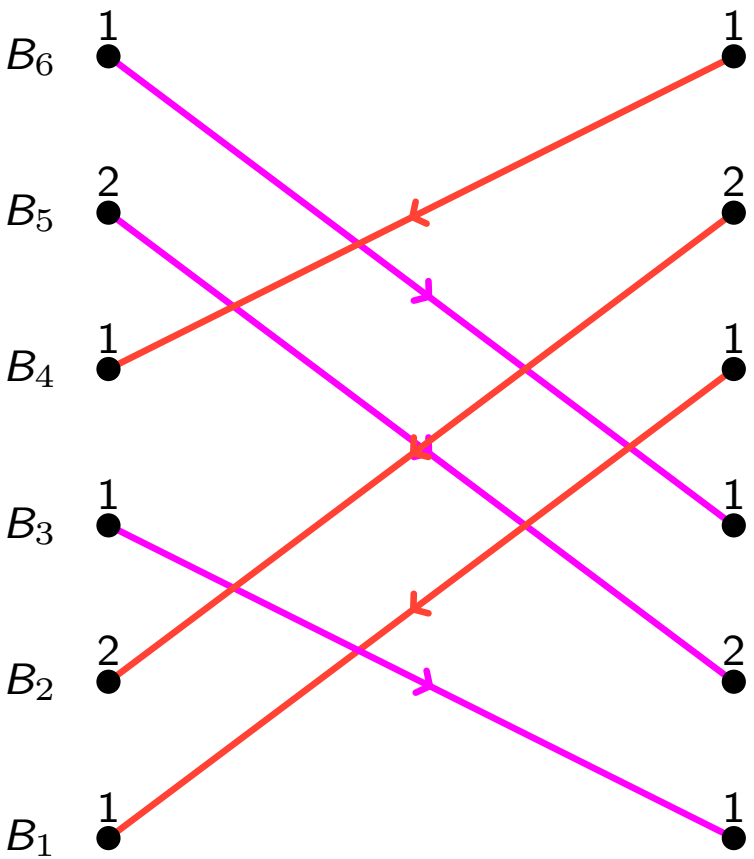
Canonical filtration

Let $D \in \mathrm{D}_n(k)$. Then the *canonical filtration* on D is the coarsest filtration $0 = D_0 \subset D_1 \subset \ldots \subset D_r = D$ such that for every i, $F(D_i) = D_j$ and $V^{-1}(D_i) = D_{j'}$ for some $j, j' \leq n$.
Set $B_i := D_i/D_{i-1}$; then for every i two options:

- $\exists \tau(i)$ such that F induces a Fr_p-semilinear $B_i \xrightarrow{\sim} B_{\tau(i)}$;
- $\exists \tau(i)$ such that V induces a Fr_p-semilinear $B_i \xleftarrow{\sim} B_{\tau(i)}$;

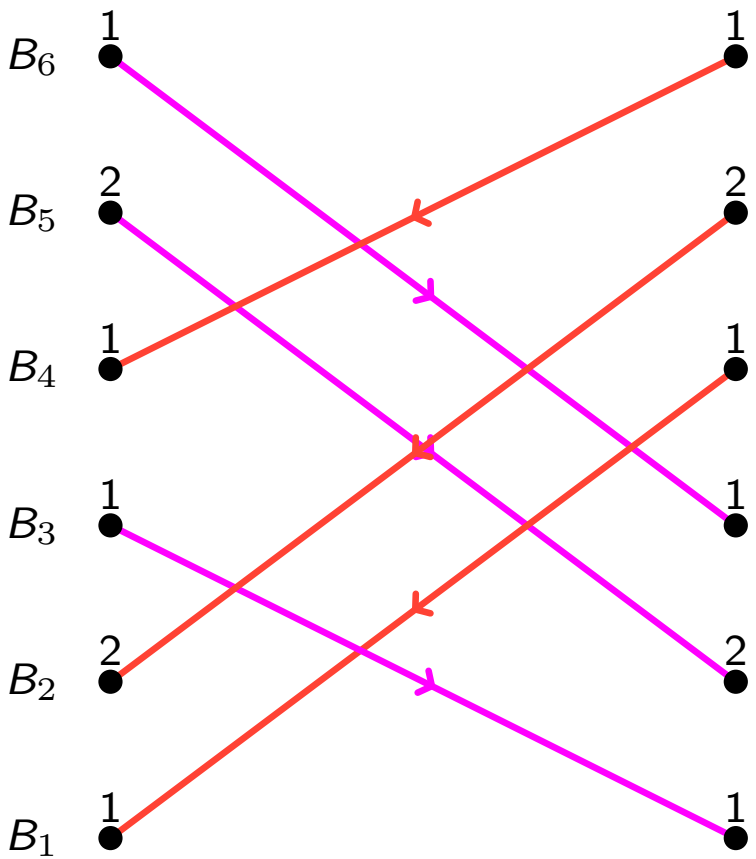
and $\tau \in S_r$.

Graph of a Dieudonné module



F, V, $\dim(B_i)$.

Graph of a Dieudonné module



F, V, $\dim(B_i)$.

Theorem

(Kraft 1975) Over $k = \bar{k}$, two Dieudonné modules with the same graph are isomorphic.

Hence there are only finitely many Dieudonné modules of dimension n over $\bar{\mathbb{F}}_p$, and we can describe them explicitely.

Automorphism group

Over $\bar{\mathbb{F}}_p$, we may assume that
Any automorphism has to fix the canonical filtration, so $\mathrm{Aut}(D)$ is a subgroup of

$$\begin{pmatrix} \mathrm{GL}(B_n) & 0 & \cdots & 0 \\ * & \mathrm{GL}(B_{n-1}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & \mathrm{GL}(B_1) \end{pmatrix}$$

Automorphism group

Over $\bar{\mathbb{F}}_p$, we may assume that
Any automorphism has to fix the canonical filtration, so $\mathrm{Aut}(D)$ is a subgroup of

$$\begin{pmatrix} \mathrm{GL}(B_n) & 0 & \cdots & 0 \\ * & \mathrm{GL}(B_{n-1}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & \mathrm{GL}(B_1) \end{pmatrix}$$

Lemma

The image H of $\mathrm{Aut}(D)$ in $\prod_i \mathrm{GL}(B_i)$ is finite.

Over $\mathbb{F}_q$

Which Dieudonné modules over $\mathbb{F}_q$ correspond to a given graph?

- Take one (D, F, V); then D defines a semilinear isomorphism $\mathrm{Fr}_q \colon D_{\bar{\mathbb{F}}_p} \to D_{\bar{\mathbb{F}}_p}$.

Over $\mathbb{F}_q$

Which Dieudonné modules over $\mathbb{F}_q$ correspond to a given graph?

- Take one (D, F, V); then D defines a semilinear isomorphism $\mathrm{Fr}_q \colon D_{\bar{\mathbb{F}}_p} \to D_{\bar{\mathbb{F}}_p}$.
- Vice versa, $D = \{d \in D_{\bar{\mathbb{F}}_p} : \mathrm{Fr}_q(d) = d\}$.

Over $\mathbb{F}_q$

Which Dieudonné modules over $\mathbb{F}_q$ correspond to a given graph?

- Take one (D, F, V); then D defines a semilinear isomorphism $\mathrm{Fr}_q \colon D_{\bar{\mathbb{F}}_p} \to D_{\bar{\mathbb{F}}_p}$.
- Vice versa, $D = \{d \in D_{\bar{\mathbb{F}}_p} : \mathrm{Fr}_q(d) = d\}$.
- Any other Dieudonné module with the same graph is obtained by 'twisting' the Frobenius action: $\tilde{\mathrm{Fr}}_q = \gamma \circ \mathrm{Fr}_q$ for some $\gamma \in \mathrm{Aut}(D_{\bar{\mathbb{F}}_p})$.

Over $\mathbb{F}_q$

Which Dieudonné modules over $\mathbb{F}_q$ correspond to a given graph?

- Take one (D, F, V); then D defines a semilinear isomorphism $\mathrm{Fr}_q \colon D_{\bar{\mathbb{F}}_p} \to D_{\bar{\mathbb{F}}_p}$.
- Vice versa, $D = \{d \in D_{\bar{\mathbb{F}}_p} : \mathrm{Fr}_q(d) = d\}$.
- Any other Dieudonné module with the same graph is obtained by 'twisting' the Frobenius action: $\tilde{\mathrm{Fr}}_q = \gamma \circ \mathrm{Fr}_q$ for some $\gamma \in \mathrm{Aut}(D_{\bar{\mathbb{F}}_p})$.
- $\gamma \sim \gamma'$ give isomorphic $D \Leftrightarrow \exists \delta \in \mathrm{Aut}(D_{\bar{\mathbb{F}}_p}) : \gamma' = \delta\gamma'\mathrm{Fr}_q(\delta)^{-1}$.

Over $\mathbb{F}_q$

Which Dieudonné modules over $\mathbb{F}_q$ correspond to a given graph?

- Take one (D, F, V); then D defines a semilinear isomorphism $\mathrm{Fr}_q \colon D_{\bar{\mathbb{F}}_p} \to D_{\bar{\mathbb{F}}_p}$.
- Vice versa, $D = \{d \in D_{\bar{\mathbb{F}}_p} : \mathrm{Fr}_q(d) = d\}$.
- Any other Dieudonné module with the same graph is obtained by 'twisting' the Frobenius action: $\tilde{\mathrm{Fr}}_q = \gamma \circ \mathrm{Fr}_q$ for some $\gamma \in \mathrm{Aut}(D_{\bar{\mathbb{F}}_p})$.
- $\gamma \sim \gamma'$ give isomorphic $D \Leftrightarrow \exists \delta \in \mathrm{Aut}(D_{\bar{\mathbb{F}}_p}) : \gamma' = \delta\gamma'\mathrm{Fr}_q(\delta)^{-1}$.
- Set $\mathrm{H}^1(\mathbb{F}_q, \mathrm{Aut}(D_{\bar{\mathbb{F}}_p})) = \mathrm{Aut}(D_{\bar{\mathbb{F}}_p})/\sim$;
- Then $\mathrm{H}^1(\mathbb{F}_q, \mathrm{Aut}(D_{\bar{\mathbb{F}}_p})) \cong \mathrm{H}^1(\mathbb{F}_q, H)$, and this can be explicitely calculated.

We can also calculate the automorphism group of the Dieudonné module corresponding to γ, and this allows us to calculate the Zeta function.

We can also calculate the automorphism group of the Dieudonné module corresponding to γ, and this allows us to calculate the Zeta function.

Research in progress:

- Zeta function for arbitrary G-zips;
- Look at $A[p^2]$ rather than $A[p]$.