Grupos p-divisibles

Piermarco Milione

STNB 2012

Introducción

Sean k un cuerpo, $c(k) = p > 0$, k^{sep} su clausura separable y $\bar{k}$ su clausura algebraica.
Sea A una variedad abeliana de dimensión g sobre k.

Introducción

Sean k un cuerpo, $c(k) = p > 0$, k^{sep} su clausura separable y $\bar{k}$ su clausura algebraica.
Sea A una variedad abeliana de dimensión g sobre k.
$\forall n \geq 0$ y primo ℓ definimos

$$A[\ell^n](k^{sep}) := \{a \in A(k^{sep}) \mid \ell^n a = 0\}$$

conjunto de puntos de ℓ^n-torsión sobre k^{sep},

Introducción

Sean k un cuerpo, $c(k) = p > 0$, k^{sep} su clausura separable y $\bar{k}$ su clausura algebraica.
Sea A una variedad abeliana de dimensión g sobre k.
$\forall n \geq 0$ y primo ℓ definimos

$$A[\ell^n](k^{sep}) := \{a \in A(k^{sep}) \mid \ell^n a = 0\}$$

conjunto de puntos de ℓ^n-torsión sobre k^{sep},
Éste es el núcleo de la isogenia

$$[\ell^n] : a \in A(k^{sep}) \longmapsto \ell^n a := a + \ldots + a \in A(k^{sep})$$

$A(\ell^n)(k^{sep})$ es un subespacio algebraico de $A(k^{sep})$ y es un grupo (abeliano) en la categoría de espacios algebraicos.

Recordamos que

- $deg[\ell^n] = \ell^{2gn}$

- $[\ell^n]$ es un morfismo étale (i.e. liso y no ramificado) $\Leftrightarrow \ell \neq p$

Recordamos que

- $deg[\ell^n] = \ell^{2gn}$

- $[\ell^n]$ es un morfismo étale (i.e. liso y no ramificado) $\Leftrightarrow \ell \neq p$

Por esto y por considerar la clausura separable del cuerpo, resulta que, cuando $\ell \neq p$,

$$A(k^{sep})[\ell^n] \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$$

Todos estos módulos $A(k^{sep})[\ell^n]$ que se obtienen al variar de n, pueden organizarse en un límite proyectivo dando lugar al *módulo de Tate de la variedad A*:

$$T_\ell(A) := \varprojlim A(k^{sep})[\ell^n]$$

Todos estos módulos $A(k^{sep})[\ell^n]$ que se obtienen al variar de n, pueden organizarse en un límite proyectivo dando lugar al *módulo de Tate de la variedad A*:

$$T_\ell(A) := \varprojlim A(k^{sep})[\ell^n]$$

Luego se ve de inmediato que hay un isomorfismo de grupos abelianos

$$T_\ell(A) \simeq (\mathbb{Z}_\ell)^{2g}$$

Todos estos módulos $A(k^{sep})[\ell^n]$ que se obtienen al variar de n, pueden organizarse en un límite proyectivo dando lugar al *módulo de Tate de la variedad A*:

$$T_\ell(A) := \varprojlim A(k^{sep})[\ell^n]$$

Luego se ve de inmediato que hay un isomorfismo de grupos abelianos

$$T_\ell(A) \simeq (\mathbb{Z}_\ell)^{2g}$$

Además sobre éste actúa de manera natural el grupo de Galois $Gal(k^{sep}/k)$.

Teorema de Tate

Sea k un cuerpo, $c(k) = p > 0$

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell[Gal(k^{sep}/k)]}(T_\ell(A), T_\ell(B))$$

es una biyección.

Teorema de Tate

Sea k un cuerpo, $c(k) = p > 0$

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell[Gal(k^{sep}/k)]}(T_\ell(A), T_\ell(B))$$

es una biyección.

- Tate conjeturó este resultado, en 1964, por un cuerpo de generación finita sobre su cuerpo primo y logró probarlo, en 1966, en el caso de un cuerpo finito.

Teorema de Tate

Sea k un cuerpo, $c(k) = p > 0$

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell[Gal(k^{sep}/k)]}(T_\ell(A), T_\ell(B))$$

es una biyección.

- Tate conjeturó este resultado, en 1964, por un cuerpo de generación finita sobre su cuerpo primo y logró probarlo, en 1966, en el caso de un cuerpo finito.
- Faltings lo demostró, en 1983, para los cuerpos de números.

Cuando $\ell = p$:

$$A(k^{sep})[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^r$$

con $0 \leq r \leq g$.
Es decir, hay menos puntos de lo esperado y esto se debe esencialmente a que la definición de variedad, en este caso, no es lo suficientemente fina como para describir completamente la situación que se presenta.

Cuando $\ell = p$:

$$A(k^{sep})[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^r$$

con $0 \leq r \leq g$.
Es decir, hay menos puntos de lo esperado y esto se debe esencialmente a que la definición de variedad, en este caso, no es lo suficientemente fina como para describir completamente la situación que se presenta.
Por esto es necesario recurrir al concepto de esquema y, más en concreto, al de *esquema en grupos conmutativo*.

Se descubre así que:

- Cuando $\ell \neq p$, $A[\ell^n]$ es un equema en grupos *étale*

Se descubre así que:

- Cuando $\ell \neq p$, $A[\ell^n]$ es un equema en grupos *étale*

- Cuando $\ell = p$, $A[p^n]$ descompone en una parte que sigue siendo étale y otra que se llamará *conexa* o *local*

Se descubre así que:

- Cuando $\ell \neq p$, $A[\ell^n]$ es un equema en grupos *étale*
- Cuando $\ell = p$, $A[p^n]$ descompone en una parte que sigue siendo étale y otra que se llamará *conexa* o *local*

La parte conexa es la que, de alguna manera recoge los puntos perdidos.

Además todos los esquemas en grupos de puntos de p^n-torsión, también se organizan en un sistema, esta vez inductivo, que da lugar a lo que definiremos como *grupo p-divisible* y que representa el comienzo para definir un análogo del módulo de Tate también en característica p y comenzar el estudio de las *variedades abelianas módulo p*.

Esquemas en grupos afines

Sea $\mathcal{C}$ una categoría cualquiera y sean X y S objetos de $\mathcal{C}$. Definimos el siguiente conjunto de morfismos en $\mathcal{C}$

$$\underline{X}(S) := \mathrm{Mor}_{\mathcal{C}}(S, X)$$

conjunto de puntos de X *a valores en* S.

Esquemas en grupos afines

Sea $\mathcal{C}$ una categoría cualquiera y sean X y S objetos de $\mathcal{C}$. Definimos el siguiente conjunto de morfismos en $\mathcal{C}$

$$\underline{X}(S) := \mathrm{Mor}_{\mathcal{C}}(S, X)$$

conjunto de puntos de X *a valores en* S.
Así, por cada X objeto de $\mathcal{C}$, hemos definido un funtor contravariante de la categoría $\mathcal{C}$ en la categoría de conjuntos $\underline{Sets}$.

$$S \in Ob(\mathcal{C}) \longmapsto \underline{X}(S) \in \underline{Sets}$$

Esquemas en grupos afines

Sea $\mathcal{C}$ una categoría cualquiera y sean X y S objetos de $\mathcal{C}$. Definimos el siguiente conjunto de morfismos en $\mathcal{C}$

$$\underline{X}(S) := \mathrm{Mor}_{\mathcal{C}}(S, X)$$

conjunto de puntos de X a valores en S.
Así, por cada X objeto de $\mathcal{C}$, hemos definido un funtor contravariante de la categoría $\mathcal{C}$ en la categoría de conjuntos $\underline{Sets}$.

$$S \in Ob(\mathcal{C}) \longmapsto \underline{X}(S) \in \underline{Sets}$$

Si consideramos la categoría $\mathcal{C}\underline{Sets}$, cuyos objetos son los funtores de $\mathcal{C}$ en $\underline{Sets}$ y cuyos morfismos son los morfismos entre funtores, entonces tenemos definido el siguiente funtor covariante:

$$X \in Ob(\mathcal{C}) \longmapsto \underline{X} := \mathrm{Mor}_{\mathcal{C}}(-, X) \in Ob(\mathcal{C}\underline{Sets})$$

Lema de Yoneda

.

El funtor $X \longmapsto \underline{X}$ es plenamente fiel.
Es decir, $\forall X, Y \in Ob(\mathcal{C})$, la aplicación natural

$$\mathrm{Mor}_{\mathcal{C}}(X, Y) \longrightarrow \mathrm{Mor}_{\mathcal{C}\underline{Sets}}(\underline{X}, \underline{Y})$$

es una biyección.

Por lo tanto la categoría $\mathcal{C}$ se puede identificar con la categoría $\mathcal{C}\underline{Sets}$, es decir es equivalente mirar a los objetos de $\mathcal{C}$ más bien que a los *conjuntos de puntos* de estos objetos.

Para dar las definiciones que siguen hay que pedir también que la categoría $\mathcal{C}$ posea el producto y el objeto final.

Para dar las definiciones que siguen hay que pedir también que la categoría $\mathcal{C}$ posea el producto y el objeto final.

Definición

Un *objeto grupo* (resp. *objeto grupo conmutativo*) en la categoría $\mathcal{C}$ es una pareja (G, μ), donde $G \in Ob(\mathcal{C})$ y $\mu \in \mathrm{Mor}_{\mathcal{C}}(G \times G, G)$ tales que para todo $S \in Ob(\mathcal{C})$ el conjunto $\underline{G}(S)$ tiene estructura de grupo (resp. grupo conmutativo) a través de la operación $\mu(S) : \underline{G}(S) \times \underline{G}(S) \to \underline{G}(S)$ definida por $\mu(S)(g, g^{'}) := \mu \circ (g, g^{'})$.

$$S \xrightarrow{(g,g)} G \times G \xrightarrow{\mu} G$$

Proposición

Sea $\mathcal{C}$ una categoría en la que existe el producto y el objeto final F. La pareja (G,μ) es un objeto grupo en la categoría $\mathcal{C}$ si y solo si valen las siguientes propiedades:

Proposición

Sea $\mathcal{C}$ una categoría en la que existe el producto y el objeto final F. La pareja (G,μ) es un objeto grupo en la categoría $\mathcal{C}$ si y solo si valen las siguientes propiedades:

(i) (Asociatividad) El siguiente diagrama conmuta:

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

Proposición

Sea $\mathcal{C}$ una categoría en la que existe el producto y el objeto final F. La pareja (G,μ) es un objeto grupo en la categoría $\mathcal{C}$ si y solo si valen las siguientes propiedades:

(i) (Asociatividad) El siguiente diagrama conmuta:

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

(ii) (Elemento neutro) Existe un morfismo de $\mathcal{C}$ $e : F \to G$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} F \times G \arrow[r, "e \times id"] \arrow[d, "pr"'] & G \times G \arrow[dl, "\mu"] \\ G & \end{tikzcd}$$

Proposición

Sea $\mathcal{C}$ una categoría en la que existe el producto y el objeto final F. La pareja (G,μ) es un objeto grupo en la categoría $\mathcal{C}$ si y solo si valen las siguientes propiedades:

(i) (Asociatividad) El siguiente diagrama conmuta:

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

(ii) (Elemento neutro) Existe un morfismo de $\mathcal{C}$ $e : F \to G$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} F \times G \arrow[r, "e\times id"] \arrow[d, "pr"'] & G \times G \arrow[dl, "\mu"] \\ G & \end{tikzcd}$$

(iii) (Simétrico de un elemento) Existe un morfismo $i : G \to G$ de manera que el siguiente diagrama conmuta:

$$\begin{tikzcd} G \times G \arrow[r, "id \times i"] & G \times G \arrow[d, "\mu"] \\ G \arrow[u, "\Delta"] \arrow[r, "f"'] & G \end{tikzcd}$$

donde Δ es la diagonal de G y f es la composición

$$G \longrightarrow F \xrightarrow{e} G\ .$$

(iii) (Simétrico de un elemento) Existe un morfismo $i : G \to G$ de manera que el siguiente diagrama conmuta:

$$\begin{tikzcd}
G \times G \arrow[r, "id \times i"] & G \times G \arrow[d, "\mu"] \\
G \arrow[u, "\Delta"] \arrow[r, "f"'] & G
\end{tikzcd}$$

donde Δ es la diagonal de G y f es la composición

$$G \longrightarrow F \xrightarrow{e} G \,.$$

(iv) (Conmutatividad) Si $\sigma : (a, b) \in G \times G \longmapsto (b, a) \in G \times G$ entonces el siguiente diagrama conmuta:

$$\begin{tikzcd}
G \times G \arrow[r, "\mu"] \arrow[d, "\sigma"'] & G \\
G \times G \arrow[ur, "\mu"'] &
\end{tikzcd}$$

El caso que estamos interesados en tratar es : $\mathcal{C} = \underline{Sch}_k$ categoría de esquemas afines sobre un anillo k

El caso que estamos interesados en tratar es : $\mathcal{C} = \underline{Sch}_k$ categoría de esquemas afines sobre un anillo k

Definición

Un *k-esquema en grupos afín conmutativo* es un objeto grupo conmutativo en la categoría de esquemas afines sobre k.

Luego, por el lema de Yoneda, es equivalente mirar a un esquema sobre k o a su conjunto de puntos.

El caso que estamos interesados en tratar es : $\mathcal{C} = \underline{Sch}_k$ categoría de esquemas afines sobre un anillo k

Definición

Un *k-esquema en grupos afín conmutativo* es un objeto grupo conmutativo en la categoría de esquemas afines sobre k.

Luego, por el lema de Yoneda, es equivalente mirar a un esquema sobre k o a su conjunto de puntos.
Por ejemplo si $X = \operatorname{Spec} k[T]$ y $S = \operatorname{Spec} k^{'}$, donde $k^{'}$ es una extensión finita cualquiera del cuerpo k, entonces el conjunto de puntos de $\operatorname{Spec} k[T]$ a valores en $\operatorname{Spec} k^{'}$ (o también a valores en $k^{'}$) es:

$$\underline{X}(S) \simeq \operatorname{Mor}_{\underline{Sch}_k}(S, X) \simeq \operatorname{Mor}_{\underline{Alg}_k}(k[T], k^{'}) \simeq k^{'}$$

Sabemos que existe una antiequivalencia

$$A \in Ob(\underline{Alg}_k) \longmapsto \mathrm{Spec} A \in Ob(\underline{Sch}_k)$$

Vamos a ver qué restricciones hay que anadir a los objetos de la categoría $\underline{Alg}_k$ para que esta antiequivalencia restrinja a una antiequivalencia en la categoría de esquemas en grupos afines conmutativos.

Recordemos que una k-álgebra A es un k-módulo junto a dos homomorfismos de k-módulos $\mu : A \otimes A \to A$ y $e : k \to A$ tales que μ es asociativa y conmutativa y e induce la unidad en A respecto de μ, i.e. $\mu(e(1) \otimes a) = a$ para todo $a \in A$.
Una vez dado un k-esquema en grupos afín conmutativo $G = \mathrm{Spec} A$, los morfismos que vienen dado con éste, corresponden a los siguientes morfismos de k-álgebras

Recordemos que una k-álgebra A es un k-módulo junto a dos homomorfismos de k-módulos $\mu : A \otimes A \to A$ y $e : k \to A$ tales que μ es asociativa y conmutativa y e induce la unidad en A respecto de μ, i.e. $\mu(e(1) \otimes a) = a$ para todo $a \in A$.
Una vez dado un k-esquema en grupos afín conmutativo $G = \mathrm{Spec} A$, los morfismos que vienen dado con éste, corresponden a los siguientes morfismos de k-álgebras

$$k \xleftarrow{\epsilon} A \xrightarrow{m} A \otimes_k A \qquad A \xrightarrow{\iota} A$$

Recordemos que una k-álgebra A es un k-módulo junto a dos homomorfismos de k-módulos $\mu : A \otimes A \to A$ y $e : k \to A$ tales que μ es asociativa y conmutativa y e induce la unidad en A respecto de μ, i.e. $\mu(e(1) \otimes a) = a$ para todo $a \in A$.
Una vez dado un k-esquema en grupos afín conmutativo $G = \mathrm{Spec} A$, los morfismos que vienen dado con éste, corresponden a los siguientes morfismos de k-álgebras

$$k \xleftarrow{\epsilon} A \xrightarrow{m} A \otimes_k A \qquad\qquad A \xrightarrow{\iota} A$$

- La aplicación m se llama *comultiplicación*

Recordemos que una k-álgebra A es un k-módulo junto a dos homomorfismos de k-módulos $\mu : A \otimes A \to A$ y $e : k \to A$ tales que μ es asociativa y conmutativa y e induce la unidad en A respecto de μ, i.e. $\mu(e(1) \otimes a) = a$ para todo $a \in A$.
Una vez dado un k-esquema en grupos afín conmutativo $G = \mathrm{Spec} A$, los morfismos que vienen dado con éste, corresponden a los siguientes morfismos de k-álgebras

$$k \xleftarrow{\epsilon} A \xrightarrow{m} A \otimes_k A \qquad A \xrightarrow{\iota} A$$

- La aplicación m se llama *comultiplicación*
- La aplicación ϵ se llama *counidad*

Recordemos que una k-álgebra A es un k-módulo junto a dos homomorfismos de k-módulos $\mu : A \otimes A \to A$ y $e : k \to A$ tales que μ es asociativa y conmutativa y e induce la unidad en A respecto de μ, i.e. $\mu(e(1) \otimes a) = a$ para todo $a \in A$.
Una vez dado un k-esquema en grupos afín conmutativo $G = \mathrm{Spec} A$, los morfismos que vienen dado con éste, corresponden a los siguientes morfismos de k-álgebras

$$k \xleftarrow{\epsilon} A \xrightarrow{m} A \otimes_k A \qquad A \xrightarrow{\iota} A$$

- La aplicación m se llama *comultiplicación*
- La aplicación ϵ se llama *counidad*
- La aplicación ι se llama *antipodismo* (o *involución*)

Definición

Una *k-biálgebra coasociativa coconmutativa counitaria y con antipodismo* (o también una *k-álgebra de Hopf coconmutativa y con antipodismo*) es una k-álgebra (conmutativa) A satisfaciendo las siguientes propiedades:

(i) m es coasociativa, i.e. $(m \otimes id) \circ m = (id \otimes m) \circ m$

(ii) m es coconmutativa, i.e. $\sigma \circ m = m$, donde $\sigma : (a, b) \in A \otimes A \longmapsto (b, a) \in A \otimes A$

(iii) ϵ es counidad respecto de m, i.e. $(\epsilon \otimes id) \circ m = 1 \otimes id$

(iv) ι es coinverso respecto de m, i.e. $e \circ \epsilon = \mu \circ (id \otimes \iota) \circ m$

Definición

Una *k-biálgebra coasociativa coconmutativa counitaria y con antipodismo* (o también una *k-álgebra de Hopf coconmutativa y con antipodismo*) es una k-álgebra (conmutativa) A satisfaciendo las siguientes propiedades:

(i) m es coasociativa, i.e. $(m \otimes id) \circ m = (id \otimes m) \circ m$

(ii) m es coconmutativa, i.e. $\sigma \circ m = m$, donde

$\sigma : (a, b) \in A \otimes A \longmapsto (b, a) \in A \otimes A$

(iii) ϵ es counidad respecto de m, i.e. $(\epsilon \otimes id) \circ m = 1 \otimes id$

(iv) ι es coinverso respecto de m, i.e. $e \circ \epsilon = \mu \circ (id \otimes \iota) \circ m$

Por lo tanto la antiequivalencia de antes restringe a una antiequivalencia de la categoría de k-álgebras de Hopf coconmutativas y con antipodismo en la categoría de esquemas en grupos afines conmutativos sobre k.

Ejemplos

(1) Se define el *k-esquema en grupos conmutativo aditivo* como el esquema afín

$$\mathbb{G}_{a,k} := \mathrm{Spec} k[T]$$

con la operación dada por la suma entre puntos de $\mathrm{Spec} k[T]$ o, equivalentemente, por el homomorfismo de k-álgebras

$$m : T \in k[T] \longmapsto T \otimes 1 + 1 \otimes T \in k[T] \otimes_k k[T],$$

Ejemplos

(1) Se define el *k-esquema en grupos conmutativo aditivo* como el esquema afín

$$\mathbb{G}_{a,k} := \mathrm{Spec} k[T]$$

con la operación dada por la suma entre puntos de $\mathrm{Spec} k[T]$ o, equivalentemente, por el homomorfismo de k-álgebras

$$m : T \in k[T] \longmapsto T \otimes 1 + 1 \otimes T \in k[T] \otimes_k k[T],$$

Resulta que para todo esquema afín $S = \mathrm{Spec} R$ el conjunto de puntos de $\mathbb{G}_{a,k}$ a valores en S es

$$\underline{\mathbb{G}}_{a,k}(S) \simeq \mathrm{Mor}_{\underline{Alg}_k}(k[T], R) \simeq R \simeq \mathcal{O}_S(S)$$

(2) Análogamente se define el *k-esquema en grupos multiplicativo* como el esquema afín

$$\mathbb{G}_{m,k} := \mathrm{Spec} k[T, T^{-1}]$$

con la operación dada por la comultiplicación $m(T) := T \otimes T$
Luego resulta que:

$$\underline{\mathbb{G}}_m(S) \simeq \mathcal{O}_S^*(S).$$

Esquemas en grupos conmutativos finitos

Definición

Un k-esquema en grupos afín G se dice *finito* sobre k si es del tipo $G = \mathrm{Spec} A$, A siendo un k-módulo localmente libre (i.e. A siendo un k-módulo proyectivo finito generado). En este caso la aplicación

$$\mathfrak{p} \in \mathrm{Spec}(k) \longmapsto dim_{k(\mathfrak{p})} A \otimes_k k(\mathfrak{p}) \in \mathbb{N}$$

(donde $k(\mathfrak{p})$ es el cuerpo de fracciones de $A/\mathfrak{p}$)
es costante y su valor en $\mathbb{N}$ es el *orden de G* sobre k.

Esquemas en grupos conmutativos finitos

Definición

Un k-esquema en grupos afín G se dice *finito* sobre k si es del tipo $G = \mathrm{Spec} A$, A siendo un k-módulo localmente libre (i.e. A siendo un k-módulo proyectivo finito generado). En este caso la aplicación

$$\mathfrak{p} \in \mathrm{Spec}(k) \longmapsto dim_{k(\mathfrak{p})} A \otimes_k k(\mathfrak{p}) \in \mathbb{N}$$

(donde $k(\mathfrak{p})$ es el cuerpo de fracciones de $A/\mathfrak{p}$)
es costante y su valor en $\mathbb{N}$ es el *orden de* G sobre k.

Dados dos esquemas en grupos finitos se define de manera obvia un homomorfismo entre ellos y luego se puede demostrar que la categoría así obtenida es abeliana.

Ejemplos

(1) *Esquema en grupos constante*:
Vamos a explicar cómo construir un esquema en grupos finito a partir de un grupo finito cualquiera.

Ejemplos

(1) *Esquema en grupos constante*:
Vamos a explicar cómo construir un esquema en grupos finito a partir de un grupo finito cualquiera.
Sea Γ un grupo conmutativo de orden r (en el sentido usual del álgebra abstracta).
Definimos el siguiente objeto en la categoría de k-esquemas afines:

Ejemplos

(1) *Esquema en grupos constante*:
Vamos a explicar cómo construir un esquema en grupos finito a partir de un grupo finito cualquiera.
Sea Γ un grupo conmutativo de orden r (en el sentido usual del álgebra abstracta).
Definimos el siguiente objeto en la categoría de k-esquemas afines:

$$\Gamma_k := \bigsqcup_{\gamma \in \Gamma} \mathrm{Spec} k$$

unión disjunta de r copias del objeto final $\mathrm{Spec} k$.

Una vez observado que

$$\Gamma_k \times \Gamma_k \simeq \coprod_{(\gamma,\gamma')\in\Gamma\times\Gamma} \mathrm{Spec} k$$

podemos definir una operación en Γ_k que al elemento $a \in \mathrm{Spec} k$ en la posición $(\gamma, \gamma') \in \Gamma \times \Gamma$ asocia el mismo elemento de $\mathrm{Spec} k$ en la posición $\gamma + \gamma'$. Resulta que Γ_k con esta operación es un esquema en grupos afín conmutativo.

Una vez observado que

$$\Gamma_k \times \Gamma_k \simeq \coprod_{(\gamma,\gamma')\in\Gamma\times\Gamma} \mathrm{Spec} k$$

podemos definir una operación en Γ_k que al elemento $a \in \mathrm{Spec} k$ en la posición $(\gamma, \gamma') \in \Gamma \times \Gamma$ asocia el mismo elemento de $\mathrm{Spec} k$ en la posición $\gamma + \gamma'$. Resulta que Γ_k con esta operación es un esquema en grupos afín conmutativo.
$\Gamma_k = \mathrm{Spec} A$ donde $A \simeq k^\Gamma$ y entonces Γ_k es un esquema en grupos finito de orden r

(2) Sea k un cuerpo, $c(k) = p > 0$. Se define el siguiente k-esquema en subgrupos de $\mathbb{G}_{a,k}$:

$$\alpha_{p,k} := \mathrm{Spec}\left(\frac{k[T]}{(T^p)}\right)$$

Resulta que para todo S esquema afín sobre k,

$$\underline{\alpha}_p(S) \simeq \{f \in \mathcal{O}_S(S) \mid f^p = 0\}$$

(2) Sea k un cuerpo, $c(k) = p > 0$. Se define el siguiente k-esquema en subgrupos de $\mathbb{G}_{a,k}$:

$$\alpha_{p,k} := \operatorname{Spec}\left(\frac{k[T]}{(T^p)}\right)$$

Resulta que para todo S esquema afín sobre k,

$$\underline{\alpha}_p(S) \simeq \{f \in \mathcal{O}_S(S) \mid f^p = 0\}$$

Este esquema en grupos se llama *k-esquema en grupos de raíces p-ésimas del cero.*

(3) De la misma manera se define también, para todo n, un k-esquema en subgrupos de $\mathbb{G}_{m,k}$:

$$\mu_{n,k} := \mathrm{Spec}\left(\frac{k[T, T^{-1}]}{(T^n - 1)}\right)$$

y luego resulta que el subgrupo de puntos a valores en S es

$$\underline{\mu}_n(S) \simeq \{f \in \mathcal{O}_S^*(S) \mid f^n = 1\}$$

(3) De la misma manera se define también, para todo n, un k-esquema en subgrupos de $\mathbb{G}_{m,k}$:

$$\mu_{n,k} := \operatorname{Spec}\left(\frac{k[T, T^{-1}]}{(T^n - 1)}\right)$$

y luego resulta que el subgrupo de puntos a valores en S es

$$\underline{\mu}_n(S) \simeq \{f \in \mathcal{O}_S^*(S) \mid f^n = 1\}$$

Este esquema se llama *k-esquema en grupos de raíces n-ésimas de la unidad*

Dualidad de Cartier

Sea R un k-álgebra de Hopf coconmutativa y con antipodismo.
Supóngase además que R sea finita.
Definimos primero $R^* := \mathrm{Hom}_k(R, k)$, dual de R como k-módulo.

Dualidad de Cartier

Sea R un k-álgebra de Hopf coconmutativa y con antipodismo. Supóngase además que R sea finita.
Definimos primero $R^* := \mathrm{Hom}_k(R, k)$, dual de R como k-módulo.
Considerando la aplicación dual de la comultiplicación

$$m : R \to R \otimes R,$$

se llega a un producto en R^*, asociativo y conmutativo,

$$m^* : R^* \otimes R^* \to R^*$$

($(R \otimes R)^* \simeq R^* \otimes R^*$, pues R es finita)

Dualidad de Cartier

Sea R un k-álgebra de Hopf coconmutativa y con antipodismo. Supóngase además que R sea finita.
Definimos primero $R^* := \mathrm{Hom}_k(R, k)$, dual de R como k-módulo.
Considerando la aplicación dual de la comultiplicación

$$m : R \to R \otimes R,$$

se llega a un producto en R^*, asociativo y conmutativo,

$$m^* : R^* \otimes R^* \to R^*$$

($(R \otimes R)^* \simeq R^* \otimes R^*$, pues R es finita)
Por lo tanto R^* resulta ser una k-álgebra de la misma dimensión que R.

Además el producto en R

$$\mu : R \otimes R \to R$$

dualiza a

Además el producto en R

$$\mu : R \otimes R \to R$$

dualiza a

$$\mu^* : R^* \to R^* \otimes R^*$$

coproducto en R^*, coasociativo y coconmutativo.

Además el producto en R

$$\mu : R \otimes R \to R$$

dualiza a

$$\mu^* : R^* \to R^* \otimes R^*$$

coproducto en R^*, coasociativo y coconmutativo.
Y también los homomorfismos de k-módulos

$$\iota : R \to R, \qquad \iota^* : R^* \to R^*$$

$$\epsilon : R \to k, \qquad \epsilon^* : \mathrm{Hom}(k, k) \simeq k \to R^*$$

dualizan corréctamennte, definiendo sobre R una estructura de álgebra de Hopf.

Definición

Para todo $G = \mathrm{Spec} A$, k-esquema en grupos conmutativo finito, está unívocamente definido un k-esquema en grupos conmutativo finito

$$G^* := \mathrm{Spec} A^*$$

que llamaremos *dual de Cartier de G* o simplemente *dual de G*.

Definición

Para todo $G = \mathrm{Spec} A$, k-esquema en grupos conmutativo finito, está unívocamente definido un k-esquema en grupos conmutativo finito

$$G^* := \mathrm{Spec} A^*$$

que llamaremos *dual de Cartier de* G o simplemente *dual de* G.

Ejemplos

Definición

Para todo $G = \mathrm{Spec} A$, k-esquema en grupos conmutativo finito, está unívocamente definido un k-esquema en grupos conmutativo finito

$$G^* := \mathrm{Spec} A^*$$

que llamaremos *dual de Cartier de* G o simplemente *dual de* G.

Ejemplos

(1) Sea Γ un grupo conmutativo finito.

$$(\Gamma_k)^* = (\mathrm{Spec}(k^\Gamma))^* = \mathrm{Spec}(k^\Gamma)^* \simeq \mathrm{Spec}(k[\Gamma])$$

donde

$$k[\Gamma] := \{\sum_{\gamma \in \Gamma} a_\gamma \cdot \gamma \mid a_\gamma \in k\}$$

Así cuando $\Gamma = \mathbb{Z}/n\mathbb{Z}$

$$(\mathbb{Z}/n\mathbb{Z})^*_k \simeq \mathrm{Spec}(k[\mathbb{Z}/n\mathbb{Z}]) \simeq \mathrm{Spec}\left(\frac{k[T]}{(T^n - 1)}\right) = \mu_{n,k}$$

Así cuando $\Gamma = \mathbb{Z}/n\mathbb{Z}$

$$(\mathbb{Z}/n\mathbb{Z})^*_k \simeq \mathrm{Spec}(k[\mathbb{Z}/n\mathbb{Z}]) \simeq \mathrm{Spec}\left(\frac{k[T]}{(T^n - 1)}\right) = \mu_{n,k}$$

(3) Del ejemplo precedente desciende que

$$(\mu_{n,k})^* \simeq (\mathbb{Z}/n\mathbb{Z})_k$$

pues el funtor de paso al dual es involutivo (i.e. $(G^*)^* \simeq G$)

Así cuando $\Gamma = \mathbb{Z}/n\mathbb{Z}$

$$(\mathbb{Z}/n\mathbb{Z})^*_k \simeq \mathrm{Spec}(k[\mathbb{Z}/n\mathbb{Z}]) \simeq \mathrm{Spec}\left(\frac{k[T]}{(T^n - 1)}\right) = \mu_{n,k}$$

(3) Del ejemplo precedente desciende que

$$(\mu_{n,k})^* \simeq (\mathbb{Z}/n\mathbb{Z})_k$$

pues el funtor de paso al dual es involutivo (i.e. $(G^*)^* \simeq G$)
(2) Se puede ver también que cuando k es un cuerpo de característica $p > 0$,

$$(\alpha_{p,k})^* \simeq \alpha_{p,k}$$

i.e. el esquema en grupos $\alpha_{p,k}$ es autodual.

Esquemas en grupos étales y conexos

Esquemas en grupos étales y conexos

En esta sección supondremos siempre que k sea un cuerpo con $\bar{k}$ su clausura algebraica y k^{sep} su clausura separable.

Esquemas en grupos étales y conexos

En esta sección supondremos siempre que k sea un cuerpo con $\overline{k}$ su clausura algebraica y k^{sep} su clausura separable.

Definición

Una k-álgebra finita A se dice *étale* si satisface una de las siguientes condiciones equivalentes :
(i) A es producto de extensiones separables de k
(ii) $A \otimes \overline{k} \simeq \overline{k}^n$ por algún entero $n \geq 1$
(iii) $A \otimes k^{sep} \simeq (k^{sep})^n$ por algún entero $n \geq 1$
(iv) $A \otimes \overline{k}$ es una $\overline{k}$-álgebra reducida (i.e. no admite elementos nilpotentes)

Defınción

Un k-esquema en grupos conmutativo finito G se dice *étale* si valen las siguientes condiciones equivalentes:

(i) $G \times_k \bar{k}$ es un esquema en grupos constante sobre $\bar{k}$

(ii) $G \times_k k^{sep}$ es un esquema en grupos constante sobre k^{sep}

(iii) El álgebra de funciones regulares de G es una k-álgebra étale

(iv) El morfismo de esquemas $G \to \mathrm{Spec}(k)$ es étale

Definción

Un k-esquema en grupos conmutativo finito G se dice *étale* si valen las siguientes condiciones equivalentes:
(i) $G \times_k \overline{k}$ es un esquema en grupos constante sobre $\overline{k}$
(ii) $G \times_k k^{sep}$ es un esquema en grupos constante sobre k^{sep}
(iii) El álgebra de funciones regulares de G es una k-álgebra étale
(iv) El morfismo de esquemas $G \to \mathrm{Spec}(k)$ es étale

El siguiente resultado pone en manifiesto la "buena propiedad" que tienen los esquemas en grupos étales.

Defnción

Un k-esquema en grupos conmutativo finito G se dice *étale* si valen las siguientes condiciones equivalentes:
(i) $G \times_k \bar{k}$ es un esquema en grupos constante sobre $\bar{k}$
(ii) $G \times_k k^{sep}$ es un esquema en grupos constante sobre k^{sep}
(iii) El álgebra de funciones regulares de G es una k-álgebra étale
(iv) El morfismo de esquemas $G \to \mathrm{Spec}(k)$ es étale

El siguiente resultado pone en manifiesto la "buena propiedad" que tienen los esquemas en grupos étales.

Teorema

El funtor

$$G \longmapsto \underline{G}(\mathrm{Spec}(k^{sep}))$$

define una equivalencia de la categoría de esquemas en grupos conmutativos étales en la categoría de grupos abelianos con una acción continua del grupo de Galois $\pi = Gal(k^{sep}/k)$.

Definición

Un k-esquema en grupos conmutativo finito G se dice *conexo* si G es conexo como espacio topológico (i.e. G no se puede expresar como la unión de dos abiertos no vacíos y disjuntos).

Definición

Un k-esquema en grupos conmutativo finito G se dice *conexo* si G es conexo como espacio topológico (i.e. G no se puede expresar como la unión de dos abiertos no vacíos y disjuntos).

Caracterizando esta propiedad respecto del anillo de funciones regulares de G se obtiene la siguiente:

Proposición

El esquema en grupos finito $G = \mathrm{Spec} A$ sobre k es conexo $\Longleftrightarrow$ A no contiene elementos idempotentes $\neq 0, 1$

Definición

Un k-esquema en grupos conmutativo finito $G = \mathrm{Spec} A$ se dice *local* si valen las condiciones equivalentes:
(i) A es una k-álgebra local.
(ii) El conjunto de puntos $\underline{G}(\mathrm{Spec} K)$ es el grupo trivial para todo cuerpo K.

Definición

Un k-esquema en grupos conmutativo finito $G = \mathrm{Spec} A$ se dice *local* si valen las condiciones equivalentes:
(i) A es una k-álgebra local.
(ii) El conjunto de puntos $\underline{G}(\mathrm{Spec} K)$ es el grupo trivial para todo cuerpo K.

Un k-esquema en grupos local es también conexo, pues un anillo local no contiene elementos idempotentes no triviales.

Definición

Un k-esquema en grupos conmutativo finito $G = \mathrm{Spec} A$ se dice *local* si valen las condiciones equivalentes:
(i) A es una k-álgebra local.
(ii) El conjunto de puntos $\underline{G}(\mathrm{Spec} K)$ es el grupo trivial para todo cuerpo K.

Un k-esquema en grupos local es también conexo, pues un anillo local no contiene elementos idempotentes no triviales.

Ejemplos

Sea k un cuerpo $c(k) = p > 0$.
El k-esquema en grupos constante $(\mathbb{Z}/p\mathbb{Z})_k$ es étale, mientras que $\mu_{p,k}$ y $\alpha_{p,k}$ son locales (y por lo tanto conexos). Sin embargo, $\mu_{p,k}$ y $\alpha_{p,k}$ no son isomorfos como esquemas en grupos finitos ya que el dual del primero es étale y el dual del segundo es local.

Dadas estas primeras definiciones se puede proceder a enunciar uno de los resultados fundamentales.

Teorema

Sean k un cuerpo cualquiera y G un esquema en grupos finito sobre k.
Entonces existe una sucesión exacta, única a menos de isomorfismos, de esquemas en grupos conmutativos finitos

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0$$

tal que G^0 es local y G^{et} es étale.

Idea de la demostración

- Sea A^{et} la k-subálgebra étale de A, maximal respecto de esta condición.

Idea de la demostración

- Sea A^{et} la k-subálgebra étale de A, maximal respecto de esta condición.
- Se prueba que $(A \otimes A)^{et} = A^{et} \otimes A^{et}$ y luego se ve fácilmente que A^{et} una k-álgebra de Hopf coconmutativa y con antipodismo.

Idea de la demostración

- Sea A^{et} la k-subálgebra étale de A, maximal respecto de esta condición.
- Se prueba que $(A \otimes A)^{et} = A^{et} \otimes A^{et}$ y luego se ve fácilmente que A^{et} una k-álgebra de Hopf coconmutativa y con antipodismo.
- Por lo tanto $G^{et} := \mathrm{Spec} A^{et}$ es un esquema en grupos étale y se tiene un homomorfismo exhaustivo de esquemas en grupos finitos $G \to G^{et}$.

Idea de la demostración

- Sea A^{et} la k-subálgebra étale de A, maximal respecto de esta condición.
- Se prueba que $(A \otimes A)^{et} = A^{et} \otimes A^{et}$ y luego se ve fácilmente que A^{et} una k-álgebra de Hopf coconmutativa y con antipodismo.
- Por lo tanto $G^{et} := \mathrm{Spec} A^{et}$ es un esquema en grupos étale y se tiene un homomorfismo exhaustivo de esquemas en grupos finitos $G \to G^{et}$.
- Luego se define $G^0 := ker(G \to G^{et})$.

Idea de la demostración

- Sea A^{et} la k-subálgebra étale de A, maximal respecto de esta condición.
- Se prueba que $(A \otimes A)^{et} = A^{et} \otimes A^{et}$ y luego se ve fácilmente que A^{et} una k-álgebra de Hopf coconmutativa y con antipodismo.
- Por lo tanto $G^{et} := \mathrm{Spec} A^{et}$ es un esquema en grupos étale y se tiene un homomorfismo exhaustivo de esquemas en grupos finitos $G \to G^{et}$.
- Luego se define $G^0 := ker(G \to G^{et})$.
- Éste es un esquema en subgrupos cerrado de G y se puede demostrar que es local (de consecuencia será conexo), pues $G = \mathrm{Spec}(A^0)$ donde A^0 es el factor local de A sobre el cual $\epsilon : A \to k$ es no nulo.

Definición

Un esquema en grupos afín se dice *reducido* si su álgebra de funciones regulares es reducida, i.e. si $G = \mathrm{Spec} A$ y A no admite elementos nilpotentes.

Definición

Un esquema en grupos afín se dice *reducido* si su álgebra de funciones regulares es reducida, i.e. si $G = \mathrm{Spec} A$ y A no admite elementos nilpotentes.

Observación

Cuando el cuerpo k es perfecto, una k-álgebra finita A es reducida si y solo si $A \otimes_k \bar{k}$ es una $\bar{k}$-álgebra reducida. Por lo tanto si G es un esquema en grupos conmutativo finito sobre un cuerpo perfecto, G reducido $\iff$ G étale

Proposición

Sea k un cuerpo perfecto y G un k-esquema en grupos conmutativo finito.

Proposición

Sea k un cuerpo perfecto y G un k-esquema en grupos conmutativo finito.
Si $G = \mathrm{Spec} A$ y $\mathfrak{N}$ es el ideal nilradical de A, entonces el anillo $A/\mathfrak{N}$ tiene una única estructura de k-álgebra de Hopf tal que la proyección $A \to A/\mathfrak{N}$ es un homomorfismo de k-álgebras de Hopf.

Proposición

Sea k un cuerpo perfecto y G un k-esquema en grupos conmutativo finito.
Si $G = \mathrm{Spec}A$ y $\mathfrak{N}$ es el ideal nilradical de A, entonces el anillo $A/\mathfrak{N}$ tiene una única estructura de k-álgebra de Hopf tal que la proyección $A \to A/\mathfrak{N}$ es un homomorfismo de k-álgebras de Hopf.

Defínción

Sea k un cuerpo perfecto y sea $G = \mathrm{Spec}A$ un k-esquema afín en grupos conmutativo. El *esquema en grupos reducido sobre k asociado a G* es el k-esquema afín en subgrupos de G

$$G_{red} := \mathrm{Spec}A_{red}$$

donde $A_{red} := A/\mathfrak{N}$ es una k-álgebra reducida.

Proposición

Sea k un cuerpo perfecto y G un k-esquema en grupos conmutativo finito.
Si $G = \mathrm{Spec} A$ y $\mathfrak{N}$ es el ideal nilradical de A, entonces el anillo $A/\mathfrak{N}$ tiene una única estructura de k-álgebra de Hopf tal que la proyección $A \to A/\mathfrak{N}$ es un homomorfismo de k-álgebras de Hopf.

Defininción

Sea k un cuerpo perfecto y sea $G = \mathrm{Spec} A$ un k-esquema afín en grupos conmutativo. El *esquema en grupos reducido sobre k asociado a G* es el k-esquema afín en subgrupos de G

$$G_{red} := \mathrm{Spec} A_{red}$$

donde $A_{red} := A/\mathfrak{N}$ es una k-álgebra reducida.
Está claro que G es reduido $\Leftrightarrow G = G_{red}$.

Teorema

Sean k un cuerpo perfecto y G un esquema en grupos conmutativo finito sobre k.
Entonces existe una sucesión exacta y escindida, única a menos de isomorfismo, de esquemas en grupos conmutativos finitos

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G_{red} \longrightarrow 0$$

tal que G^0 es local y G_{red} es el esquema en grupos reducido asociado a G.

Dem.

Dem.

- Ocurre demostrar que el homomorfismo $G_{red} \hookrightarrow G \to G/G^0$ es un isomorfismo de esquemas en grupos sobre k.

Dem.

- Ocurre demostrar que el homomorfismo $G_{red} \hookrightarrow G \to G/G^0$ es un isomorfismo de esquemas en grupos sobre k.
- G_{red} es étale y por lo tanto $G_{red} \times_k k^{sep}$ es un k^{sep}-esquema en grupos constante.

Dem.

- Ocurre demostrar que el homomorfismo $G_{red} \hookrightarrow G \to G/G^0$ es un isomorfismo de esquemas en grupos sobre k.
- G_{red} es étale y por lo tanto $G_{red} \times_k k^{sep}$ es un k^{sep}-esquema en grupos constante.
- Luego se ve que el homomorfismo $G_{red} \times k^{sep} \to (G/G^0) \times k^{sep}$ es una biyección entre dos esquemas en grupos constantes sobre k^{sep}

Dem.

- Ocurre demostrar que el homomorfismo $G_{red} \hookrightarrow G \to G/G^0$ es un isomorfismo de esquemas en grupos sobre k.
- G_{red} es étale y por lo tanto $G_{red} \times_k k^{sep}$ es un k^{sep}-esquema en grupos constante.
- Luego se ve que el homomorfismo $G_{red} \times k^{sep} \to (G/G^0) \times k^{sep}$ es una biyección entre dos esquemas en grupos constantes sobre k^{sep}
- Entonces es un isomorfismo de esquemas en grupos étales sobre k^{sep}.

Dem.

- Ocurre demostrar que el homomorfismo $G_{red} \hookrightarrow G \to G/G^0$ es un isomorfismo de esquemas en grupos sobre k.
- G_{red} es étale y por lo tanto $G_{red} \times_k k^{sep}$ es un k^{sep}-esquema en grupos constante.
- Luego se ve que el homomorfismo $G_{red} \times k^{sep} \to (G/G^0) \times k^{sep}$ es una biyección entre dos esquemas en grupos constantes sobre k^{sep}
- Entonces es un isomorfismo de esquemas en grupos étales sobre k^{sep}.
- Los funtores $G \longmapsto G_{red}$ y $G \longmapsto G^0$ son compatibles respecto de extensiones de k y luego podemos suponer $k = k^{sep}$.

Dado un esquema en grupos finito G. Denotamos por G_{xy} un esquema en subgrupos de G tal que G es x, G^* es y. Tomamos además la convención: r=reducido y l=local. Luego podemos enunciar el siguiente

Dado un esquema en grupos finito G. Denotamos por G_{xy} un esquema en subgrupos de G tal que G es x, G^* es y.
Tomamos además la convención: r=reducido y l=local.
Luego podemos enunciar el siguiente

Teorema

Sea k un cuerpo perfecto y G un esquema en grupos conmutativo finito sobre k.
Entonces G descompone de la siguiente manera, única a menos de isomorfismos, en producto de esquemas en subgrupos:

$$G \simeq G_{rr} \times G_{rl} \times G_{lr} \times G_{ll}$$

Proposición

Supongamos que G es un esquema en grupos finito simple sobre un cuerpo k de característica $p > 0$ (i.e. no existe ningún k-esquema en sugrupos finito de G no trivial).
La siguiente tabla describe las posibles clases de isomorfía de G sobre su clausura separable k^{sep}, con sus representantes y sus órdenes.

Proposición

Supongamos que G es un esquema en grupos finito simple sobre un cuerpo k de característica $p > 0$ (i.e. no existe ningún k-esquema en sugrupos finito de G no trivial).
La siguiente tabla describe las posibles clases de isomorfía de G sobre su clausura separable k^{sep}, con sus representantes y sus órdenes.

Clase de isomorfía	Representante de la clase	Orden
reducido-reducido	$(\mathbb{Z}/\ell\mathbb{Z})_{k^{sep}}$	$\ell \neq p$
reducido-local	$(\mathbb{Z}/p\mathbb{Z})_{k^{sep}}$	p
local-reducido	$\mu_{p,k^{sep}}$	p
local-local	$\alpha_{p,k^{sep}}$	p

Esquema en grupos de puntos de n-torsión

Sea X un esquema abeliano de dimensiń g sobre el cuerpo k, $c(k) = p > 0$ (i.e. un esquema en grupos X sobre k, propio y liso, cuyas fibras geométricas son conexas y de dimensión g) y sea $n = p^f m$ un entero positivo, con $f \geq 0$, $m \geq 1$ y $(p, m) = 1$. El objetivo que nos proponemos es analizar la estructura del esquema en subgrupos finito $X_n := \mathrm{Ker}[n]_X$. Supongamos además que $k = k^{sep}$

Esquema en grupos de puntos de n-torsión

Sea X un esquema abeliano de dimensiń g sobre el cuerpo k, $c(k) = p > 0$ (i.e. un esquema en grupos X sobre k, propio y liso, cuyas fibras geométricas son conexas y de dimensión g) y sea $n = p^f m$ un entero positivo, con $f \geq 0$, $m \geq 1$ y $(p, m) = 1$.
El objetivo que nos proponemos es analizar la estructura del esquema en subgrupos finito $X_n := \mathrm{Ker}[n]_X$. Supongamos además que $k = k^{sep}$

- $X_n \simeq X_m \times X_{p^r}$ donde

Esquema en grupos de puntos de n-torsión

Sea X un esquema abeliano de dimensiń g sobre el cuerpo k, $c(k) = p > 0$ (i.e. un esquema en grupos X sobre k, propio y liso, cuyas fibras geométricas son conexas y de dimensión g) y sea $n = p^f m$ un entero positivo, con $f \geq 0$, $m \geq 1$ y $(p, m) = 1$. El objetivo que nos proponemos es analizar la estructura del esquema en subgrupos finito $X_n := \mathrm{Ker}[n]_X$. Supongamos además que $k = k^{sep}$

- $X_n \simeq X_m \times X_{p^r}$ donde $X_m \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$ de orden $2gm$, componente de tipo reducido-reducido .

Esquema en grupos de puntos de n-torsión

Sea X un esquema abeliano de dimensiń g sobre el cuerpo k, $c(k) = p > 0$ (i.e. un esquema en grupos X sobre k, propio y liso, cuyas fibras geométricas son conexas y de dimensión g) y sea $n = p^f m$ un entero positivo, con $f \geq 0$, $m \geq 1$ y $(p, m) = 1$. El objetivo que nos proponemos es analizar la estructura del esquema en subgrupos finito $X_n := \mathrm{Ker}[n]_X$. Supongamos además que $k = k^{sep}$

- $X_n \simeq X_m \times X_{p^r}$ donde
  $X_m \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$ de orden $2gm$, componente de tipo reducido-reducido .
  X_{p^f} de orden p^{2gf}, producto de las componentes reducido-local, local-reducido y local-local.

Esquema en grupos de puntos de n-torsión

Sea X un esquema abeliano de dimensiń g sobre el cuerpo k, $c(k) = p > 0$ (i.e. un esquema en grupos X sobre k, propio y liso, cuyas fibras geométricas son conexas y de dimensión g) y sea $n = p^f m$ un entero positivo, con $f \geq 0$, $m \geq 1$ y $(p, m) = 1$.
El objetivo que nos proponemos es analizar la estructura del esquema en subgrupos finito $X_n := \mathrm{Ker}[n]_X$. Supongamos además que $k = k^{sep}$

- $X_n \simeq X_m \times X_{p^r}$ donde
  $X_m \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$ de orden $2gm$, componente de tipo reducido-reducido .
  X_{p^f} de orden p^{2gf}, producto de las componentes reducido-local, local-reducido y local-local.
- Supongamos

  $$X_{p,red} \simeq (\mathbb{Z}/p\mathbb{Z})^r$$

  por algún entero $r \geq 0$.

- Por consideraciones de órdenes

$$X_{p^f,red} = (X_n)_{rl} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r$$

- Por consideraciones de órdenes

$$X_{p^f,red} = (X_n)_{rl} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r$$

- Luego se puede demostrar que el dual $(X_{p^f})^*$ es núcleo del morfismo de multiplicación por p^ν en el dual X^*.

- Por consideraciones de órdenes

$$X_{p^f,red} = (X_n)_{rl} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r$$

- Luego se puede demostrar que el dual $(X_{p^f})^*$ es núcleo del morfismo de multiplicación por p^ν en el dual X^*.
- Por lo tanto

$$(X_{p^f})^*_{red} \simeq (\mathbb{Z}/p^f\mathbb{Z})^s$$

por algún entero $s \geq 0$

- Por consideraciones de órdenes

$$X_{p^f,red} = (X_n)_{rl} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r$$

- Luego se puede demostrar que el dual $(X_{p^f})^*$ es núcleo del morfismo de multiplicación por p^ν en el dual X^*.
- Por lo tanto

$$(X_{p^f})^*_{red} \simeq (\mathbb{Z}/p^f\mathbb{Z})^s$$

por algún entero $s \geq 0$

- Pasando de nuevo al dual,

$$(X_n)_{lr} \simeq \mu^s_{p^f,k}$$

- $X_{p^f} \simeq (\mathbb{Z}/p^f\mathbb{Z})_k^r \times \mu_{p^f,k}^s \times (X_{p^f})_{ll}$

- $X_{p^f} \simeq (\mathbb{Z}/p^f\mathbb{Z})_k^r \times \mu_{p^f,k}^s \times (X_{p^f})_{ll}$
- Como X_{p^f} tiene orden p^{2gf} resulta que

$$(X_{p^f})_{ll} \simeq \alpha_{p^f,k}^t$$

por un entero $t \geq 0$ tal que $r + s + t = 2g$.

- $X_{p^f} \simeq (\mathbb{Z}/p^f\mathbb{Z})_k^r \times \mu_{p^f,k}^s \times (X_{p^f})_{ll}$
- Como X_{p^f} tiene orden p^{2gf} resulta que

$$(X_{p^f})_{ll} \simeq \alpha_{p^f,k}^t$$

  por un entero $t \geq 0$ tal que $r + s + t = 2g$.
- Luego se puede probar que los enteros $r = r_X, s = s_X, t = t_X$ son invariantes por la clase de isogenia de X y de esto descende $r_X = r_{X^*} = s_X$.

- $X_{p^f} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r_k \times \mu^s_{p^f,k} \times (X_{p^f})_{ll}$
- Como X_{p^f} tiene orden p^{2gf} resulta que

$$(X_{p^f})_{ll} \simeq \alpha^t_{p^f,k}$$

  por un entero $t \geq 0$ tal que $r + s + t = 2g$.
- Luego se puede probar que los enteros $r = r_X, s = s_X, t = t_X$ son invariantes por la clase de isogenia de X y de esto descende $r_X = r_{X^*} = s_X$.
- $$X_{p^f} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r_k \times \mu^r_{p^f,k} \times \alpha^t_{p^f,k}$$

  donde $t \geq 0$ tal que $2r + t = 2g$.

- $X_{p^f} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r_k \times \mu^s_{p^f,k} \times (X_{p^f})_{ll}$
- Como X_{p^f} tiene orden p^{2gf} resulta que

$$(X_{p^f})_{ll} \simeq \alpha^t_{p^f,k}$$

  por un entero $t \geq 0$ tal que $r + s + t = 2g$.
- Luego se puede probar que los enteros $r = r_X, s = s_X, t = t_X$ son invariantes por la clase de isogenia de X y de esto descende $r_X = r_{X^*} = s_X$.
- $$X_{p^f} \simeq (\mathbb{Z}/p^f\mathbb{Z})^r_k \times \mu^r_{p^f,k} \times \alpha^t_{p^f,k}$$

  donde $t \geq 0$ tal que $2r + t = 2g$.

El entero $0 \leq r \leq g$ se llama *p-rango de X*.

Grupos p-divisibles

Grupos p-divisibles

Vamos a presentar dos definiciones equivalentes de grupo p-divisible

La primera requiere el importante concepto de esquema en grupos formal.

Grupos p-divisibles

Vamos a presentar dos definiciones equivalentes de grupo p-divisible

La primera requiere el importante concepto de esquema en grupos formal.

Supongamos que k sea un cuerpo.

Grupos p-divisibles

Vamos a presentar dos definiciones equivalentes de grupo p-divisible

La primera requiere el importante concepto de esquema en grupos formal.

Supongamos que k sea un cuerpo.

Definición

Un *esquema en grupos formal sobre k* es un límite directo de esquemas en grupos conmutativos finitos sobre k, i.e. G es un k-esquema en grupos formal si y solo si existe una familia de k-esquemas en grupos finitos $\{G_i\}_{i\in I}$ tal que para todo esquema afín $S = \mathrm{Spec} B$

$$\underline{G}(S) = \varinjlim \underline{G_i}(S)$$

El grupo formal explicado por Manin

El grupo formal explicado por Manin

- En la teoría clásica, un grupo de Lie simple y conexo puede ser reconstruido de manera única a partir de su grupo de Lie local.

El grupo formal explicado por Manin

- En la teoría clásica, un grupo de Lie simple y conexo puede ser reconstruido de manera única a partir de su grupo de Lie local.
- La correspondencia entre grupos algebraicos y grupos formales es análoga a la correspondencia entre grupos de Lie globales y grupos de Lie locales.

El grupo formal explicado por Manin

- En la teoría clásica, un grupo de Lie simple y conexo puede ser reconstruido de manera única a partir de su grupo de Lie local.
- La correspondencia entre grupos algebraicos y grupos formales es análoga a la correspondencia entre grupos de Lie globales y grupos de Lie locales.
- Ésta se basa en el hecho que el elemento neutro de un grupo algebraico es un punto no singular. Por lo tanto toda función algebraica definida sobre el grupo y regular en el elemento neutro se puede expresar como una serie formal de potencias en n parámetros, donde $n = \dim(G)$.

El grupo formal explicado por Manin

- En la teoría clásica, un grupo de Lie simple y conexo puede ser reconstruido de manera única a partir de su grupo de Lie local.
- La correspondencia entre grupos algebraicos y grupos formales es análoga a la correspondencia entre grupos de Lie globales y grupos de Lie locales.
- Ésta se basa en el hecho que el elemento neutro de un grupo algebraico es un punto no singular. Por lo tanto toda función algebraica definida sobre el grupo y regular en el elemento neutro se puede expresar como una serie formal de potencias en n parámetros, donde $n = \dim(G)$.
- Así, obtenemos una ley de grupo en el grupo algebraico; el grupo formal así definido se llama compleción de G.

Definición 1 (de grupo p-divisible)

Definición 1 (de grupo p-divisible)

Sea p un primo y h un entero no negativo.
Un *grupo p-divisible sobre k de altura h* (o también *grupo de Barsotti-Tate*) es un k-esquema en grupos conmutativo formal G satisfaciendo las siguiente propiedades:

(i) $[p]_G : G \to G$ es un epimorfismo de esquemas en grupos formales

(ii) $\mathrm{Ker}\,([p]_G)$ es un esquema en grupos finito de orden p^h sobre k.

(iii) $G = \varinjlim \mathrm{Ker}([p^\nu]_G)$

Definición 2 (de grupo p-divisible)

Definición 2 (de grupo p-divisible)

Sea p un primo y h un entero no negativo.
Un *grupo p-divisible sobre k de altura h* es un sistema inductivo

$$G = \varinjlim (G_\nu, i_\nu)$$

tal que para todo $\nu \geq 0$ se teien que:
(i) G_ν es un k-esquema en grupos finito de orden $p^{\nu h}$
(ii) $i_\nu : G_\nu \to G_{\nu+1}$ es una inmersión cerrada de esquemas en grupos finitos
(iii) la sucesión

$$0 \longrightarrow G_\nu \xrightarrow{i_\nu} G_{\nu+1} \xrightarrow{[p^\nu]} G_{\nu+1}$$

es exacta (i.e. G_ν se puede identificar por medio de i_ν con el núcleo de la multiplicación por p^ν en $G_{\nu+1}$)

Observación

Obsérvese que si los esquemas en grupos G_ν fuesen "simplemente" grupos abelianos los axiomas implicarían

$$G = \varinjlim G_\nu = \varinjlim \left(\mathbb{Z}/p^\nu\mathbb{Z}\right)^h = \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^h$$

Observación

Obsérvese que si los esquemas en grupos G_ν fuesen "simplemente" grupos abelianos los axiomas implicarían

$$G = \varinjlim G_\nu = \varinjlim \left(\mathbb{Z}/p^\nu\mathbb{Z}\right)^h = \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^h$$

Ejemplo

Sea X un esquema abeliano sobre k de dimensíon relativa g. Para todo entero $\nu \geq 1$

Observación

Obsérvese que si los esquemas en grupos G_ν fuesen "simplemente" grupos abelianos los axiomas implicarían

$$G = \varinjlim G_\nu = \varinjlim \left(\mathbb{Z}/p^\nu\mathbb{Z}\right)^h = \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^h$$

Ejemplo

Sea X un esquema abeliano sobre k de dimensíon relativa g. Para todo entero $\nu \geq 1$

- X_{p^ν} es el núcleo del morfismo $X \xrightarrow{[p^\nu]} X$

Observación

Obsérvese que si los esquemas en grupos G_ν fuesen "simplemente" grupos abelianos los axiomas implicarían

$$G = \varinjlim G_\nu = \varinjlim \left(\mathbb{Z}/p^\nu\mathbb{Z}\right)^h = \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^h$$

Ejemplo

Sea X un esquema abeliano sobre k de dimensíon relativa g. Para todo entero $\nu \geq 1$

- X_{p^ν} es el núcleo del morfismo $X \xrightarrow{[p^\nu]} X$
- $i_\nu : X_{p^\nu} \hookrightarrow X_{p^{\nu+1}}$ la inclusión,

Observación

Obsérvese que si los esquemas en grupos G_ν fuesen "simplemente" grupos abelianos los axiomas implicarían

$$G = \varinjlim G_\nu = \varinjlim \left(\mathbb{Z}/p^\nu\mathbb{Z}\right)^h = \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^h$$

Ejemplo

Sea X un esquema abeliano sobre k de dimensíon relativa g. Para todo entero $\nu \geq 1$

- X_{p^ν} es el núcleo del morfismo $X \xrightarrow{[p^\nu]} X$
- $i_\nu : X_{p^\nu} \hookrightarrow X_{p^{\nu+1}}$ la inclusión,

Entonces $X(p) := \varinjlim(X_{p^\nu}, i_\nu)$ es un grupo p-divisible de altura $h = 2g$.
(pues cada X_{p^ν} es un esquema en grupos finito de orden $p^{2g\nu}$ sobre k).

Definición

Si en la definición de grupo p-divisible cada esquema en grupos G_ν es étale (resp. conexo / reducido / local) entonces se dice que *el grupo p-divisible G es étale* (resp. *conexo* / *reducido* / *local*).

Definición

Si en la definición de grupo p-divisible cada esquema en grupos G_ν es étale (resp. conexo / reducido / local) entonces se dice que *el grupo p-divisible G es étale* (resp. *conexo* / *reducido* / *local*).

Dado un grupo p-divisible $G = (G_\nu, i_\nu)$ y aplicando el teorema de la sucesión local-étale a cada uno de los esquemas en grupos finitos G_ν se obtiene una sucesión exacta, además única a menos de isomorfismo, de grupos p-divisibles:

Definición

Si en la definición de grupo p-divisible cada esquema en grupos G_ν es étale (resp. conexo / reducido / local) entonces se dice que *el grupo p-divisible G es étale* (resp. *conexo* / *reducido* / *local*).

Dado un grupo p-divisible $G = (G_\nu, i_\nu)$ y aplicando el teorema de la sucesión local-étale a cada uno de los esquemas en grupos finitos G_ν se obtiene una sucesión exacta, además única a menos de isomorfismo, de grupos p-divisibles:

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0$$

donde G^{et} es un grupo p-divisible étale y G^0 es un grupo p-divisible conexo.

Definición

Si en la definición de grupo p-divisible cada esquema en grupos G_ν es étale (resp. conexo / reducido / local) entonces se dice que *el grupo p-divisible G es étale* (resp. *conexo* / *reducido* / *local*).

Dado un grupo p-divisible $G = (G_\nu, i_\nu)$ y aplicando el teorema de la sucesión local-étale a cada uno de los esquemas en grupos finitos G_ν se obtiene una sucesión exacta, además única a menos de isomorfismo, de grupos p-divisibles:

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0$$

donde G^{et} es un grupo p-divisible étale y G^0 es un grupo p-divisible conexo.

Evidentemente será:

$$G^{et} = \varinjlim (G_\nu^{et}, i_\nu) \qquad G^0 = \varinjlim (G_\nu^0, i_\nu)$$

con las inclusiones i_ν oportunamente restringidas en ambos casos.

Por lo que concerne los grupos p-divisibles étales resulta que, estos ya están clasificados

De echo es equivalente dar el grupo p-divisible étale $G = \varinjlim G_\nu$ o el módulo galoisiano $T(G) := \varprojlim \left(\underline{G_\nu} \, (k^{sep}) \right)$, limite inverso de grupos abelianos, todos con una acción de $Gal(k^{sep}/k)$.

Por lo que concerne los grupos p-divisibles étales resulta que, estos ya están clasificados
De echo es equivalente dar el grupo p-divisible étale $G = \varinjlim G_\nu$ o el módulo galoisiano $T(G) := \varprojlim \left(G_\nu\,(k^{sep})\right)$, limite inverso de grupos abelianos, todos con una acción de $Gal(k^{sep}/k)$.
Así mismo, cuando k es un cuerpo finito de caracteríastica p, ℓ un primo $\neq p$ y X un esquema abeliano de dimensión g sobre k, el grupo ℓ-divisible $X(\ell)$ sobre k es étale y resulta que $X(p)$ es equivalente al módulo de Tate

$$T_\ell(X) := \varprojlim \left(X_{\ell^n}(k^{sep})\right)$$

con acción del grupo de Galois, como ha sido definido en la introducción.

Luego hace falta clasificar los grupos p-divisibles conexos.
Primero necesitamos la siguiente

Definición

Luego hace falta clasificar los grupos p-divisibles conexos. Primero necesitamos la siguiente

Definición

Sea k un cuerpo de caracteríastica $p \neq 0$.
Un *grupo formal de Lie conmutativo de dimensión n sobre k* es una pareja Γ=$(\mathcal{A}, m^*)$ donde

- $\mathcal{A} = k[[X_1, ..., X_n]]$
- $m^* : \mathcal{A} \longrightarrow \mathcal{A}\hat{\otimes}\mathcal{A} \simeq k[[Y_1, ..., Y_n, Z_1, ..., Z_n]]$ homomorfismo de anillos

satisfaciendo los axiomas que se encontrarán a continuacíń.

Una vez observado que el homomorfismo se define por una familia de n series de potencias en $2n$ variables,

$$F(Y,Z) = ((f_i(Y,Z))_{i=1,\ldots,n}$$

los axiomas se expresan de la siguiente manera:

Una vez observado que el homomorfismo se define por una familia de n series de potencias en $2n$ variables,

$$F(Y, Z) = ((f_i(Y, Z))_{i=1,\ldots,n}$$

los axiomas se expresan de la siguiente manera:

- $X = F(X, 0) = F(0, X)$ (*elemento neutro*)
- $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (*asociativivdad*)
- $F(X, Y) = F(Y, X)$ (*conmutatividad*)

Una vez observado que el homomorfismo se define por una familia de n series de potencias en $2n$ variables,

$$F(Y,Z) = ((f_i(Y,Z))_{i=1,\ldots,n}$$

los axiomas se expresan de la siguiente manera:

- $X = F(X,0) = F(0,X)$ (*elemento neutro*)
- $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (*asociativivdad*)
- $F(X,Y) = F(Y,X)$ (*conmutatividad*)

Ahora, puesto $X * Y := F(X,Y)$ definimos un homomorfismo $\psi : \mathcal{A} \to \mathcal{A}$ dado por $\psi(X) := X * \ldots * X$ (p veces), multiplicación por p en $\mathcal{A}$.
Diremos que el grupo formal de Lie Γ es *divisible* si ψ es una isogenia (i.e. exhaustiva y con núcleo finito).

Teorema

Sea k un cuerpo de caracteríastica $p \neq 0$.
Entonces existe una equivalencia entre la categoría de grupos formales de Lie conmutativos sobre k que son divisibles y la categoría de grupos p-divisibles conexos sobre k.

Teorema

Sea k un cuerpo de caracteríastica $p \neq 0$.
Entonces existe una equivalencia entre la categoría de grupos formales de Lie conmutativos sobre k que son divisibles y la categoría de grupos p-divisibles conexos sobre k.

Idea de la demostración

Vamos a ver cuál es la correspondencia que da lugar a esta equivalencia.
Dado un grupo formal de Lie conmutativo y divisible $\Gamma = (\mathcal{A}, m^*)$, definimos para todo $\nu \geq 0$
$\Gamma_{p^\nu} := \mathrm{Spec} A_\nu$ donde $A_\nu := \mathcal{A}/\psi^\nu(X_1, ..., X_n)\mathcal{A}$
Luego A_ν es un anillo local y por lo tanto Γ_{p^ν} es un esquema en grupos conexo.

Así, definiendo

$$\Gamma(p) := \varinjlim \Gamma_{p^\nu}$$

(respecto de las inclusiones obvias) se obtiene un grupo p-divisible conexo.
Además los Γ_{p^ν} han sido definidos como núcleos de morfismos de multiplicación por p^ν en $\mathcal{A}$ (los homomorfismos ψ^ν) y se sabe que cada uno de estos morfismo tiene grado $\left(p^h\right)^\nu$ donde p^h es el grado de ψ. Por lo tanto resulta que los Γ_{p^ν} son esquemas en grupos finitos de orden $p^{h\nu}$ y luego la altura de $\Gamma(p)$ es $h = log_p\,(deg\psi)$.
La asociación así definida

$$\Gamma \longmapsto \Gamma(p)$$

es una equivalencia entre las dos categorías consideradas.

Referéncias

- van der Geer, G; Moonen, B.: *Abelian Varieties* (preliminary version of the first chapters). http://staff.science.uva.nl/ bmoonen/boek/BookAV.html
- Manin, Yu.I., Theory of commutative formal groups over fields of finite characteristic. *Uspehi Mat. Nauk*, 18, 1963, no. 6, (114), 3-90.
- Milne, James S.: *Abelian varieties*. Marzo 2008, http://www.jmilne.org/math/CourseNotes/AV.pdf.
- Milne, James S.: *Algebraic groups, Lie groups and their Arithmetic subgroups*. Abril 2011, http://www.jmilne.org/math/CourseNotes/ALA.pdf.

- Mumford, David: *Abelian varieties.* With appendices by C. P. Ramanujam and Yuri Manin. Corrected reprint of the second (1974) edition. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi.
- Pink, Richard: *Finite group schemes*. Lecture course in WS 2004/05, http://www.math.ethz.ch/ pink/ftp/.../TitleContents.pdf
- Serre, J-P.: Groupes p-divisibles (d'après J. Tate). *Séminaire Bourbaki*, 19e année, 1966/67, n. 318.
- Tate, J. T.: p-divisible groups. 1967 *Proc. Conf. Local Fields* (Driebergen, 1966) pp. 158–183 Springer, Berlin.

- Waterhouse, William C.: Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.* (4) 2 1969 521–560.
- Waterhouse, W. C.; Milne, J. S.: Abelian varieties over finite fields. 1969 Number Theory Institute (*Proc. Sympos. Pure Math.*, Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), pp. 53–64. Amer. Math. Soc., 1971.