Módulos de Drinfeld sobre campos

Héctor Pastén

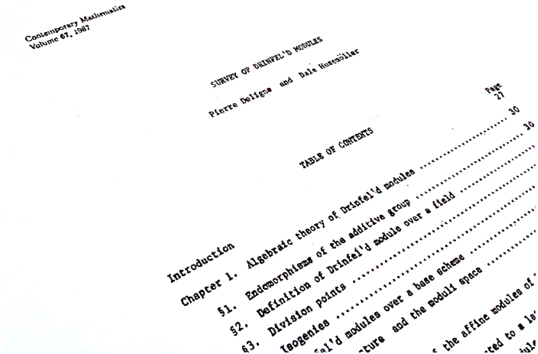
Pontificia Universidad Católica de Chile

2021/04/21

Referencia

Ahora que ya tenemos una noción de qué son los módulos de Drinfeld y para qué sirven, vamos a estudiar algunos capítulos de

P. Deligne, D. Husemöller, *Survey of Drinfel'd modules*. Contemporary Mathematics, vol 67, 1987.


Contemporary Mathematics
Volume 67, 1987

SURVEY OF DRINFEL'D MODULES

Pierre Deligne and Dale Husemöller

TABLE OF CONTENTS

El grupo aditivo

Dado un anillo R, el **grupo aditivo** sobre R es el funtor

$$G_{a,R} : \mathbf{Alg_R} \to \mathbf{AbGp}$$

que a cada R-álgebra S le asocia el grupo aditivo $G_{a,R}(S) = (S, +)$.

- Cuando R está claro, simplemente se anota G_a.
- El funtor $G_{a,R}$ es representado por $R[X]$:

$$Mor_R(R[X], S) \leftrightarrow S.$$

Un morfismo de funtores $\phi : G_a \to G_a$ está representado por un morfismo $\phi : R[X] \to R[X]$, i.e. por el polinomio $\phi(X)$. No cualquier polinomio sirve, ya que ϕ preserva la estructura de grupo.

La condición correcta es que ϕ sea **aditivo**: $\phi(X + Y) = \phi(X) + \phi(Y)$

Endomorfismos del grupo aditivo

Proposición. La construcción anterior da una biyección

$$End_R(G_a) \to \{\phi(X) \in R[X] : \phi(X) \text{ es aditivo}\}.$$

Ejemplos.

- Sea $a \in R$. Dada cualquier R-álgebra S tenemos el morfismo de grupos aditivos $S \to S$ dado por $s \mapsto as$. Corresponde al polinomio $aX \in R[X]$.
- Suponga que p es un número primo con $pR = 0$. Dada cualquier R-álgebra S tenemos el morfismo aditivo $s \mapsto s^p$. Corresponde la polinomio $X^p \in R[X]$

Proposición. Sea k un campo. Consideramos el caso $R = k$.

- Si $\mathrm{char}(k) = 0$ entonces $\mathrm{End}_k(G_a) = \{cX : c \in k\}$.
- Si $\mathrm{char}(k) = p$ entonces los polinomios aditivos sobre k son todos los de la forma $\phi(X) = c_0X + c_1X^p + c_2X^{p^2} + ... + c_nX^{p^n}$.

Polinomios torcidos

La biyección $End_R(G_a) \to \{\phi(X) \in R[X] : \phi(X) \text{ es aditivo}\}$ es un isomorfismo de anillos (no-abelianos en general) con la suma y la composición. El neutro es Id que corresponde a $\phi(X) = X$. Desde ahora identificamos estos anillos.

En lo que sigue fijamos k campo de característica $p > 0$.

El anillo de **polinomios torcidos** $k\{\tau\}$ como grupo aditivo es $k[\tau]$ pero lo dotamos del producto

$$\tau a = a^p \tau.$$

Proposición. La función $\theta : \mathrm{End}_k(G_a) \to k\{\tau\}$ dada por

$$\theta(a_0 X + a_1 X^p + ... + a_n X^{p^n}) = a_0 + a_1 \tau + ... + a_n \tau^n$$

es un isomorfismo de anillos. Se anota $\widetilde{\phi}(\tau) := \theta(\phi(X))$.

Grado, altura y derivadas

(1) Funciones **grado** de polinomio:

- $\deg : \mathrm{End}_k(G_a) \to \mathbb{Z}$, $\deg(a_0 X + \dots + a_n X^{p^n}) = p^n$
- $d : k\{\tau\} \to \mathbb{Z}$, $d(a_0 + a_1\tau + \dots + a_n\tau^n) = n$.

Relación: $\deg(\phi(X)) = p^{d(\widetilde{\phi}(\tau))}$.

(2) Funciones **altura** (no confundir con "altura de punto racional"):

- $\mathrm{ht} : \mathrm{End}_k(G_a) \to \mathbb{Z}$, $\mathrm{ht}(a_h X^{p^h} + \dots + a_n X^{p^n}) = h$ si $a_h \neq 0$
- $\mathrm{ht} : k\{\tau\} \to \mathbb{Z}$, $\mathrm{ht}(a_h\tau^h + \dots + a_n\tau^n) = h$ idem.

Relación: $\mathrm{ht}(\phi(X)) = \mathrm{ht}(\widetilde{\phi}(\tau))$. Notar que $\mathrm{ht} = \mathrm{ord}_\tau$ en $\mathrm{End}_k(G_a)$.

(3) **Derivadas** (en realidad no derivamos nada...)

- $\partial_0 : \mathrm{End}_k(G_a) \to k$, $\partial_0(a_0 X + \dots + a_n X^{p^n}) = a_0$
- $\partial : k\{\tau\} \to k$, $\partial(a_0 + \dots + a_n\tau^n) = a_0$.

Relación: $\partial_0(\phi(X)) = \partial(\widetilde{\phi}(\tau))$.

Construyendo polinomios aditivos

Lema. Sea $H \subseteq G_a(k)$ subgrupo (aditivo) finito. El polinomio $P_H(X) = \prod_{h \in H}(X - h)$ es aditivo.
Así, $P_H \in \mathrm{End}_k(G_a)$ y tenemos $H = \ker(P_H)(k)$.

Dem. Sea Y una variable y sea $Q(X) = P_H(X + Y) - P_H(Y) \in k(Y)[X]$. Notar que $Q(h) = 0$ para todo $h \in H$ porque H es grupo. Comparando grados y ceros llegamos a $Q(X) = P_H(X)$. O sea

$$P_H(X) = P_H(X + Y) - P_H(Y). \quad \square$$

Notación para campos de funciones

- k sigue siendo un campo de característica $p > 0$.
- q es una potencia de p.
- C es una curva suave, proyectiva, geométricamente irreducible, definida sobre $\mathbb{F}_q$.
- ∞ es un punto cerrado de C.
- $A = \mathcal{O}_C(C - \{\infty\})$.
- $|-|_\infty$ valor absoluto asociado a v_∞, normalizado por $|a|_\infty = \#A/a$ para todo $0 \neq a \in A$

Ejemplo. $C = \mathbb{P}^1_{\mathbb{F}_q}$, $\infty = [0:1]$.
Sea $T = x_1/x_0$ en $\mathbb{P}^1_{\mathbb{F}_q}$, entonces $A = \mathbb{F}_q[T]$ y $|a|_\infty = q^{\deg(a)}$ para $a \in A$.

Observaciones sobre $\phi : A \to End_k(G_a)$

Un módulo de Drinfeld sobre k para la curva puntada (C, ∞) será cierto tipo de morfismo de anillo

$$\phi : A \to \mathrm{End}_k(G_a).$$

O sea, ϕ da una manera en la que G_a se convierte en un A-módulo. Pero no todo ϕ servirá. Vamos a pedir ϕ **inyectivo** debido a lo siguiente:

- Si $\phi : A \to \mathrm{End}_k(G_a) \simeq k\{\tau\}$ no es inyectivo, $\ker(\phi)$ es maximal (A es dominio de Dedekind) así que $\mathrm{im}(\phi)$ es campo. Luego, $\mathrm{im}(\phi) \subseteq k \subseteq k\{\tau\}$. Este caso no es interesante.
- Definimos $\|a\|_\phi = \deg(\phi(a))$. Esto es $A \to \mathrm{End}_k(G_a) \to \mathbb{Z}$. Entonces $\| - \|_\phi$ cumple los axiomas de valor absoluto no-arquimediano en A y $\|a\|_\phi \geq 1$ para todo $0 \neq a \in A$. Por lo que $\| - \|_\phi$ o bien es trivial, o bien $\|x\|_\phi = |x|_\infty^r$ para cierto $r > 0$
- $\| - \|_\phi$ es trivial $\Leftrightarrow \mathrm{im}(\phi) \subseteq k \subseteq k\{\tau\} \Leftrightarrow \phi$ no es inyectiva.

Módulos de Drinfeld sobre k

Un **módulo de Drinfeld** sobre k para la curva puntada (C, ∞) es un morfismo inyectivo de anillos

$$\phi : A \to \mathrm{End}_k(G), \qquad \text{con } G \simeq G_a.$$

Así, $\| - \|_\phi = | - |_\infty^r$ para cierto $r > 0$, que llamaremos **rango** de ϕ.

Proposición (se demostrará más adelante). r es entero.

Punto de vista funtorial

Dado un módulo de Drinfeld $\phi : A \to \mathrm{End}_k(G_a)$ tenemos el funtor

$$E : \mathbf{Alg}_k \longrightarrow \mathbf{Mod}_A.$$

dado por $E(S) =$ el grupo aditivo $G_a(S)$ con la estructura de A-módulo determinada por ϕ.

Morfismos de módulos de Drinfeld

Sean $\phi : A \to \mathrm{End}_k(G)$ y $\phi' : A \to \mathrm{End}_k(G')$ módulos de Drinfeld. Un **morfismo** es un $u : G \to G'$ tal que para todo $a \in A$ tenemos

$$\phi'_a \circ u = u \circ \phi_a.$$

- u corresponde a un morfismo de funtores $E \to E'$.
- Si $u : G \to G'$ no es el morfismo trivial que manda todo al neutro, entonces decimos que u es una **isogenia**.

Comparación bajo isogenia

Proposición. Sea $u : \phi \to \phi'$ isogenia entre módulos de Drinfeld $\phi, \phi' : A \to \mathrm{End}_k(G_a)$. Entonces $r = r'$.

Dem. Notar que $u \in \mathrm{End}_k(G_a)$. Tenemos

$$\|a\|_{\phi'} \deg u = \deg(\phi'_a u) = \deg(u\phi_a) = \deg(u)\|a\|_{\phi}.$$

Concluimos por la definición de rango. □