Una primera introducción a los módulos de Drinfeld

Héctor Pastén

Pontificia Universidad Católica de Chile

2021/03/24

Analogía entre $\mathbb{Q}$ y $\mathbb{F}_q(T)$

En esta charla $\mathbb{F}_q$ es un campo finito de característica p con $q = p^r$ elementos, y T es una variable. Escribimos $K = \mathbb{F}_q(T)$ y $A = \mathbb{F}_q[T]$.

Aspectos análogos entre $\mathbb{Q}$ y K:

- Enteros: $\mathbb{Z}$ y $A = \mathbb{F}_q[T]$
- Sistema completo de valores absolutos:

$$M_{\mathbb{Q}} = \{\text{primos}\} \cup \{\infty\}, \quad M_K = \{f \in A : \text{irred}\} \cup \{1/T\}$$

- Campos residuales son finitos: $\mathbb{Z}/\ell\mathbb{Z} = \mathbb{F}_\ell$, $A/(f) = \mathbb{F}_{q^{\deg(f)}}$
- Ecuaciones diofantinas: Coeficientes y soluciones en $\mathbb{Q}$ o $\mathbb{Z}$ para el caso numérico, en K o A en el caso funcional.

Ejemplo. Sea $p > 3$ y sea $E : y^2 = x(x + T)(x + T^p)$. Esto define una curva elíptica sobre K. Tenemos el punto K-racional $(1, (1 + T)^{(p+1)/2})$:

$$1 \cdot (1 + T) \cdot (1 + T^p) = (1 + T)(1 + T)^p = (1 + T)^{p+1} = y^2.$$

Diferencias entre $\mathbb{Q}$ y K

¡Muchas! de partida, $\mathbb{Q}$ tiene característica 0 y K tiene característica p.

Pero una diferencia clave para lo que haremos es que el valor absoluto al infinito de $\mathbb{Q}$ es Arquimediano

$$|x|_\infty = |x|_{usual}$$

mientras que el de K es el valor absoluto asociado a $1/T$, o sea

$$|x|_\infty = q^{\deg(x)}$$

que es **no-Arquimediano**

¿Qué queremos hacer?

Queremos algo sobre $K = \mathbb{F}_q(T)$ que sea un buen sustituto de las curvas elípticas que existen sobre $\mathbb{Q}$.

- Podríamos usar curvas elípticas sobre K. Eso está bien y es muy útil en algunos casos: hay un teorema de Mordell-Weil, puntos de torsión, módulo de Tate, función L, conjetura BSD (demostrada en varios casos), etc.
- Pero en otros casos las curvas elípticas sobre K no producen lo que uno quisiera. Por ejemplo, sus espacios de moduli son simplemente reducciones módulo p de las curvas modulares clásicas. No da una teoría genuinamente sobre K de formas modulares.
- Los **módulos de Drinfeld** son un objeto matemático distinto pero que consigue hacer sobre K lo que las curvas elípticas hacen sobre $\mathbb{Q}$ en varios aspectos importantes (por ejemplo, sus espacios de moduli dan una buena teoría de formas modulares.)

¿Por dónde comenzar?

Hay varias formas de presentar las curvas elípticas:

- Elemental: plana con ley cuerda-tangente
- Algebraico: curva proyectiva de género 1 con punto racional distinguido
- Analítico: Toros complejos, retículos en $\mathbb{C}$, Función $\wp$ de Weierstrass.
- General: partir hablando de grupos algebraicos y darlas como ejemplo
- Etc.

Cada presentación tiene sus ventajas, y después se reconcilian entre ellas.

Ejemplo. Si queremos hablar de curvas modulares $X_\Gamma = \Gamma\backslash\mathfrak{h}^*$ conviene el punto de vista de retículos (analítico) para entender X_Γ como espacio de moduli.

Pero después hay que hacerlo algebraico para poder hablar campos de definición de X_Γ ("una curva elíptica E con Γ-estructura definida sobre F corresponde a un punto F-racional de X_Γ")

¿Por dónde comenzar?

Con módulos de Drinfeld (que no hemos definido todavía) ocurre lo mismo.

Para empezar a hablar de ellos hay que elegir qué tipo de presentación haremos, y después reconciliarla con otros puntos de vista.

Hoy comenzaremos con un punto de vista analítico basado en retículos.

Detalle importante.

- Sobre $\mathbb{Q}$ el punto de vista analítico de curvas elípticas comienza con retículos en $\mathbb{C} = (\mathbb{Q}_\infty)^{alg}$. Esto es un campo arquimediano.
- Nosotros usaremos retículos en $F = (K_\infty)^{alg}$ que es un campo **no-arquimediano**. ¡El análisis (convergencia de series y productos) es mucho más sencillo que en $\mathbb{C}$!

El campo $F = (K_\infty)^{alg}$

$K_\infty = \mathbb{F}_q((1/T))$ es completo, no es algebraicamente cerrado, y contiene a $A = \mathbb{F}_q[T]$ de forma discreta.
"Discreto" en detalle: para todo $B > 0$ el siguiente conjunto es finito:

$$\{x \in A : |x|_\infty \leq B\} = \{x \in A : \deg(x) \leq \log_q(B)\}.$$

Análogo: $\mathbb{R} = \mathbb{Q}_\infty$ es completo, no es algebraicamente cerrado, y contiene a $\mathbb{Z}$ de forma discreta.

¡Cuidado! la analogía se rompe al tomar clausura algebraica:

- $F = (K_\infty)^{alg}$ es algebraicamente cerrado, de grado infinito sobre K_∞, y no es completo con respecto al valor absoluto extendido desde K_∞.
- $\mathbb{C} = (\mathbb{Q}_\infty)^{alg}$ es algebraicamente cerrado, de grado 2 sobre $\mathbb{Q}_\infty = \mathbb{R}$, y es completo con respecto al valor absoluto extendido desde $\mathbb{R}$.

Retículos en $F = (K_\infty)^{alg}$

Recordar. Un retículo en $\mathbb{C}$ es un $\mathbb{Z}$-módulo $M \subseteq \mathbb{C}$ que es discreto en la topología de $\mathbb{C}$.
Hay de rango 0, 1 y 2. Los de rango 2 dan curvas elípticas $\mathbb{C}/M$.

Definición. Un retículo $M \subseteq F$ es un A-módulo que es finitamente generado y discreto.

- M es f.g. sobre A que es DIP. Además $M_{tor} = (0)$ porque $M \subseteq F$. Así que $M \simeq A^{t_M}$ como A-módulos donde $t_M = \mathrm{rk}_A(M)$.
- Como M es f.g., el campo intermedio $L_M = K_\infty(M) \subseteq F$ es finito sobre K_∞. Así que es completo.

Ejemplos.

- $M = A \subseteq K_\infty \subseteq F$ es un retículo. Cumple $t_M = 1$ y $L_M = K_\infty$.
- $M = A[\sqrt{T}]$ es un retículo de rango 2. Es discreto porque $\sqrt{T} \notin K_\infty = \mathbb{F}_q((1/T))$. Cumple $L_M = K_\infty(\sqrt{T})$.

Nota. A diferencia de $\mathbb{C}$, en F hay retículos de rango cualquiera.

Función "exponencial"

Sea $M \subseteq F$ retículo. Se define $e_M : F \to F$ como el producto

$$e_M(x) = x \cdot \prod_{0 \neq m \in M} \left(1 - \frac{x}{m}\right)$$

Propiedades básicas

- e_M converge absoluta y uniformemente sobre compactos en todo F porque M es discreto (convergencia no-arquimediana solo necesita que el factor tienda a 1).
- e_M es analítica, dada por una serie de potencias con coeficientes en L_M.
- A priori esto justifica convergencia en la completación de F, pero como los coeficientes están en L_M, para todo $x \in F$ tenemos $e_M(x) \in L_M(x) \subseteq F$.

Función "exponencial"

Sea $M \subseteq F$ retículo. Se define $e_M : F \to F$ como el producto

$$e_M(x) = x \cdot \prod_{0 \neq m \in M} \left(1 - \frac{x}{m}\right)$$

Propiedades más técnicas

- (Drinfeld) La función $e_M : F \to F$ es $\mathbb{F}_q$-lineal.
- $\ker(e_M) = M$
- $e_M : F \to F$ es sobreyectiva: viene del análisis no-arquimediano, no es tan específico de e_M.
- Obtenemos un isomorfismo $\mathbb{F}_q$-lineal $e_M : F/M \to F$.

Como F/M es A-módulo, ahora F adquiere una nueva estructura de A-módulo. Esto es un módulo de Drinfeld.

Ideas para la proxima charla (¿voluntario?)

Plan:

- Demostrar la $\mathbb{F}_q$-linealidad
- Versión algebraica de módulo de Drinfeld: Describir la acción exótica de A (que depende de la elección de M) en F directamente.
- Ejemplos.