Drinfeld Modules

Colin Olairez

December 2024

1 Motivation

Drinfeld modules were created by Vladimir Drinfeld in 1974, who was able to utilize them in proving the Langlands conjectures in some special cases. Drinfeld later introduced a generalization of Drinfeld modules through the shtuka, and used shtukas of rank 2 to prove even more cases of the Langlands conjecture. Overall, Drinfeld Modules are an important object in modern number theory.

2 Notation

The following is the notation that will be used for the remainder of the talk:

F_q = A finite field with q elements, where q is a power of the prime p.

$A = F_q[T]$

$\mathfrak{p}$ = A nonzero prime ideal of A.

3 The Ring of Twisted Polynomials

Let K be a field, and let x,y be indeterminates. A polynomial is additive if the equality:

$f(x+y) = f(x) + f(y)$ holds in $K[x, y]$.

Let F_q be a subfield of K. $f(x) \in K[x]$ is F_q-linear if $f(x)$ is additive and $f(\alpha x) = \alpha f(x)$ for $\alpha \in F_q$. $f(x) \in K[x]$ is F_q-linear iff it is of the form:

$\sum a_i x^{q^i}$, $a_i \in K$

We denote the set of F_q-linear polynomials by $K\langle x\rangle$.

One can define a different version of this ring through the following construction:

$K\{\tau\}$ = The set of polynomials $\sum a_i \tau^i$, $a_i \in K$. To define multiplication of elements of this ring, first let:

$(c\tau^i)(d\tau^j) = cd^{q^i}\tau^{i+j}$

and extend this to all other polynomials via the distributive laws.

This is indeed a different version of $K\langle x\rangle$ as it is possible to define the isomorphism:

$$\iota : K\{\tau\} \to K\langle x\rangle$$
$$\sum a_i \tau^i \mapsto \sum a_i x^{q^i}$$

By abuse of notation, denote $\iota(f) = f(x)$.

4 Definition of the Drinfeld Module

An A-field is a field K along with a homomorphism $\gamma : A \to K$. From here on out, let K be an A-field.

A Drinfeld module of rank $r \geq 1$ over K is a homomorphism:

$$\begin{aligned} \phi &: A \to K\{\tau\} \\ &a \mapsto \phi_a = \gamma(a) + g_1(a)\tau^i + \cdots + g_n(a)\tau^n \end{aligned}$$

Where for $a \neq 0$ we have:

$n = deg(a) * r$ and $g_n(a) \neq 0$. We can denote this Drinfeld module by ϕ.

The reason these are called Drinfeld modules and not Drinfeld homomorphisms is because the existence of ϕ allows one to derive a brand new A-module structure through the action:

$a * k = \phi_a(k)$ where $a \in A$, $k \in K$. This is the F_q-linear polynomial $\phi_a(x)$ evaluated at k.

Refer to this new A-module by ${}^{\phi}K$.

5 Isogenies of Drinfeld Modules

Let ϕ and ψ be Drinfeld modules over K. With these Drinfeld modules comes the A-modules ${}^{\phi}K$ and ${}^{\psi}K$. Applying the definition of module homomorphisms leads us to define a **morphism** $u : \phi \to \psi$ of Drinfeld modules as a polynomial $u \in K\{\tau\}$ such that:

$u\phi_a = \psi_a u$ for all $a \in A$.

A nonzero morphism is an **isogeny**. Additionally, given this isogeny u, one can discover an isogeny $\hat{u} : \psi \to \phi$ where $u\hat{u} = \phi_a$ for some $a \in A$. This is the **dual** of u.

6 Torsion Points of Drinfeld Modules and the Tate Module

If ϕ is a Drinfeld module of rank $r \geq 1$ over K, Let $\phi[a]$ be the roots of $\phi_a(x)$ for $a \in A$, $a \neq 0$. $\phi[a]$ has a natural A-module structure defined by $\beta * \alpha = \phi_\beta(\alpha)$, $\beta \in A$, $\alpha \in \phi[a]$. Take a prime $\mathfrak{p}$ and consider $\phi[\mathfrak{p}^n]$.

There is a surjective homomorphism, $\phi[\mathfrak{p}^n] \to \phi[\mathfrak{p}^{n-1}]$ given by $\alpha \to \phi_\mathfrak{p}(\alpha)$. One can take the inverse limit with respect to these maps, to reach the $\mathfrak{p}$-adic **Tate module** of ϕ.

$T_\mathfrak{p}(\phi) = \varprojlim_n \phi[\mathfrak{p}^\mathfrak{n}]$.

If $u : \phi \to \psi$ is an isogeny of Drinfeld modules over K, then u also induces a map of their respective Tate modules.

$u_\mathfrak{p} : T_\mathfrak{p}(\phi) \to T_\mathfrak{p}(\psi)$

Lastly, consider the Galois group $G = Gal(K^{sep}/K)$ of K. Each element of G can be thought of as acting on $\phi[a]$, as these elements permute the roots of $\phi_a(x)$. One can also directly compute that this action commutes with the action of A on $\phi[a]$.

One can even derive a representation of the Galois group G:

$\hat{\rho}_{\phi,\mathfrak{p}} : G \to Aut_{A_\mathfrak{p}}(T_\mathfrak{p}(\phi)) \cong GL_r(A_\mathfrak{p})$

7 Drinfeld Modules over a Finite Field and the Frobenius

If we now define the A-field K to specifically be F_{q^n}, we can relate the theory of Drinfeld modules and the Frobenius automorphism, $Fr_k \in G$ of $\bar{k}$. Define:

$\hat{\rho}_{\phi,\mathfrak{p}}(x) = det(x - \hat{\rho}_{\phi,\mathfrak{p}}(Fr_k)) \in A_{\mathfrak{p}}[x]$ as the characteristic polynomial of $\hat{\rho}_{\phi,\mathfrak{p}(Fr_k)}$; the characteristic polynomial of the Frobenius.

Investigating the properties of the characteristic polynomial of the Frobenius reveals significant information about Drinfeld modules over a finite field. As an example:

Two Drinfeld modules ϕ and ψ are isogenous iff their Frobenius characteristic polynomials are equal.