INTRODUCTION TO THE ALGEBRAIC THEORY OF DRINFELD MODULES

MIKAYEL MKRTCHYAN

Let me know if you find any mistakes! Our approach primarily follows Flicker's book "Drinfeld Moduli Schemes and Automorphic Forms: The Theory of Elliptic Modules With Applications".

1. Subgroups of $\mathbb{G}_a$

Let L be a characteristic p field.

Proposition 1.1. Any subgroup scheme H of $\mathbb{G}_{a,L}$ equals $\ker P$ for a unique monic $P \in L[\tau]$. The fppf quotient $\mathbb{G}_{a,L}/H$ is isomorphic to $\mathbb{G}_{a,L}$.

Proof. The subgroup H corresponds to some ideal $(f) \subset L[x]$, and it can be seen via the Hopf algebra viewpoint that it has the desired form. It is clear that the map $P : \mathbb{G}_{a,L} \to \mathbb{G}_{a,L}$ is surjective in the fppf topology. □

Proposition 1.2. Let $f, g \in L[\tau]$ be such that the corresponding additive polynomials $f(x)$ and $g(x)$ (obtained by replacing τ by x^p) satisfy $g(x)|f(x)$. Then there exists an additive polynomial $h \in L[\tau]$ such that $f = hg$.

The utility of this proposition is that divisibility of polynomials can be directly checked via their kernels (i.e. roots).

Proof. One reduces to the case where g is separable; we further assume that f and g are monic. Consider $\ker(g)$ and $\ker(f)$ as subgroups of $\overline{L}$. We have that $\ker(g) \subset \ker(f)$, and in fact $g : \overline{L} \to \overline{L}$ defines a bijection $\ker(f) \simeq \ker(f)/\ker(g)$. Thus we can view $\ker(f)/\ker(g)$ as a $\mathrm{Gal}(\overline{L}/L)$-invariant finite subgroup of $\overline{L}$. Let $h = \prod_{a \in \ker(f)/\ker(g)}(x - a)$; this is an additive polynomial. By examining their roots we have that $g(x) = h(f(x))$ and hence $g = hf \in \overline{L}[\tau]$; finally, it is clear that h has coefficients in L. □

2. Drinfeld modules

Let X be a smooth, proper, geometrically connected curve over $\mathbb{F}_q$. Fix a closed point $\infty \in |X|$, and let $A = \mathcal{O}(X \setminus x)$ be the ring of functions regular away from ∞.

Definition 2.1. Let L be a field equipped with a map $i : L \to A$. A *Drinfeld module* over L is a map $\varphi : A \to L[\tau]$ such that the composition $A \to L[\tau] \xrightarrow{D} L$ equals i, where $D : L[\tau] \to L$ is the constant term map, and φ is not the inclusion $A \xrightarrow{i} L \to L[\tau]$, where the last map is the inclusion as the constants. The *characteristic* of L is the place $v \in |\operatorname{Spec} A|$ that is the kernel of i.

Proposition 2.2. For any Drinfeld module $\phi : A \to L[\tau]$, ϕ is injective.

Proof. Otherwise the image of ϕ would be a subfield, and in particular would consist of invertible elements; however $(L[\tau])^\times = L^\times$, contradicting the condition in the definition of a Drinfeld module. □

Let (i, ϕ) be a Drinfeld module over L. There is a degree map $\deg : L[\tau] \to \mathbb{N}$ sending $\sum_{i=0}^{n} a_i \tau^i$ to p^i. This map satisfies $\deg(fg) = \deg(f)\deg(g)$ and $\deg(f+g) \leq \max(\deg(f), \deg(g))$. This implies that the composition $\deg \circ \phi : A \to \mathbb{N}$ is a valuation on A, necessarily corresponding to the place ∞: this implies that there exists some r such that $\deg(\varphi(a)) = |a|_\infty^r$. (Here we are using the normalized valuation at ∞, i.e. a function with pole of order 1 would have valuation equal to the size of the residue field at ∞.)

Definition 2.3. The unique $r \in \mathbb{Q}$ such that $\deg(\varphi(a)) = |a|_\infty^r$ is called the *rank* of the Drinfeld module φ).

In the analogy between A and $\mathbb{Z}$, the analogous notion for $\mathbb{Z}$ gives $\mathbb{G}_a$ rank 0, $\mathbb{G}_m$ rank 1 and an elliptic curve E rank 2. This rank can be understood as the dimension of the lattice by which we need to quotient $\mathbb{G}_a$ to obtain the group (so analytically, $\mathbb{G}_m$ is the quotient of $\mathbb{G}_a$ by $\mathbb{Z}$ via the exponential, and similarly an elliptic curve is the quotient by a rank 2 lattice). More algebraically, it can also be deduced from the number of torsion points: in each case the N-torsion subgroups are isomorphic (over the algebraic closure) to $(\mathbb{Z}/N)^{\text{rank}}$, at least away from the characteristic in the case of an elliptic curve.

Both these viewpoints generalize to Drinfeld modules; let us concentrate on the latter.

Proposition 2.4. Let (i, φ) be a Drinfeld module over L, and let $I \subset X$ be an ideal such that $V(I) \cap \operatorname{char}(L) = \emptyset$. Then the I-torsion subgroup in $\overline{L}$ is isomorphic to $(A/I)^r$, where r is the rank of φ.

Proof. It suffices to prove the result for a power of I; by finiteness of the class group of A, there is some power $I^h = (b)$ that is principal. The fact that $V(I) \cap \operatorname{char}(L) = \emptyset$ implies that $\varphi(b)$ is separable, i.e. has non-zero constant term. This implies that the b-torsion subgroup in $\overline{L}$ has $\deg(\varphi(b)) = |b|_\infty^r$ points. Similarly the b^2-torsion subgroup has $|b|_\infty^{2r}$ points. The result follows from the following simple lemma:

Lemma 2.5. Let M be a finite $A/(b^2)$-module, and let $M_a \subset M$ be the submodule annihilated by a. Then $\#M \leq \#M_a^2$, and equality holds if and only if M is a free $A/(b^2)$-module.

□

Corollary 2.6. For any $v \in |\operatorname{Spec} A| \setminus \operatorname{char}(L)$, the v-adic Tate module of φ is a free A_v-module of rank r.

3. Isogenies

Given a Drinfeld module φ over an A-field L, let us think of the additive group $E := \mathbb{G}_{a,L}$ over L as an A-module via φ.

Definition 3.1. Let (E, φ) and (E', φ') be Drinfeld modules over L. An *isogeny* from E to E' is some $P \in L[\tau]$ such that $P : E \to E'$ intertwines the A-actions, i.e. for any $a \in A$, $\varphi'(a)P = P\varphi(a)$. The set of all isogenies will be denoted by $\mathrm{Hom}_A(E, E')$.

Upon looking at degrees it is immediate that non-zero isogenies exist only between modules of the same rank. Let us call an isogeny f *separable* if it has non-zero constant term.

Proposition 3.2. Let (E, φ) and (X', φ') be Drinfeld modules over an A-field L, and $f : X \to X'$ be a non-zero isogeny.

(1) If $\mathrm{char}(L) = 0$, then f is separable.

(2) If $\mathrm{char}(L) = v \in |\operatorname{Spec} A|$, let q_v denote the size of the residue field of A at v. Then it is possible to write $f = g\tau^m$ so that p^m is a power of q_v, and g is separable. Moreover, there exists another Drinfeld module (X'', φ'') over L such that τ^m defines an isogeny $X \to X''$ and g defines an isogeny $X'' \to X'$.

Proof. (1) Let $c\tau^m$ be the smallest degree summand in f. Equating the smallest degree terms in $\varphi'(a)P = P\varphi(a)$ gives $c\tau^m i(a) = i(a)c\tau^m$ and hence $i(a)^{p^m} = i(a)$. If $m \neq 0$, this implies that the image of $i : A \to L$ is contained in a finite subfield, contradicting the characteristic 0 assumption.

(2) The same proof implies that p^m is a power of q_v: indeed, we must have $b^{p^m} = b$ for all $b \in \mathbb{F}_{q_v}$. We define (X'', φ'') as follows: if $\varphi(a) = \sum a_i \tau^i$, let $\varphi''(a) = a_i^{p^m} \tau^i$. We then have that τ^m is an isogeny from X to X'': indeed, for any a the equation

$$(\sum a_i^{p^m} \tau^i)\tau^m = \tau^m (\sum a_i \tau^i)$$

follows directly from the commutation relation. To prove that g defines an isogeny $X'' \to X'$, note that for any $a \in A$, $\varphi'(a)g\tau^m = g\tau^m\varphi(a) = g\varphi''(a)\tau^m$. Since $L[\tau]$ has no zero-divisors, we obtain $\varphi'(a)g = g\varphi''(a)$. □

□

Given an isogeny $f : X \to X'$, the above proposition implies constraints on $\ker(f)$: if $\mathrm{char}(L) = 0$ then $\ker(f)$ is reduced, and if $\mathrm{char}(L) = v$ then the connected part of $\ker(f)$ equals $\operatorname{Spec} k[t]/(t^{q_v^j})$ for some j.

Proposition 3.3. Conversely, a finite subgroup scheme $H \subset X$ is the kernel of an isogeny $X \to X'$ for some Drinfeld module (X', φ') over L if and only if $H(\overline{L}) \subset X(\overline{L})$ is an A-submodule, and the connected part H_{loc} is either trivial if $\mathrm{char}(L) = 0$ or equals $\operatorname{Spec} k[t]/(t^{q_v^j})$ for some j if $\mathrm{char}(L) = v$.

Proof. One direction was proved above. Conversely, assuming the conditions on H, let $f \in L[\tau]$ be the unique monic polynomial whose kernel is H. It suffices to treat the separable and purely inseparable cases separately. In the purely inseparable case $f = \tau^m$, the same construction as in part (2) of the previous proposition gives us (E', φ'). If f is separable, for any $a \in A$ consider $\psi(a) = f\varphi(a)$. The fact that $H(\overline{L})) \subset X(\overline{L})$ is A-invariant implies that $\psi(a)$ vanishes on $H(\overline{L})$; since f is separable, by Proposition 1.2 this implies that $\psi(a)$ is divisible by f, i.e. $\psi(a) = \varphi'(a)f$ for some $\varphi'(a) \in L[\tau]$. Then $\varphi'(a)$ is the desired elliptic module. □

Corollary 3.4. Given an isogeny $f : X \to X'$, there exists an isogeny $f' : X' \to X$ such that $g \circ f = \varphi(b)$ for some $b \in A$.

Proof. We can write $f = g\tau^m$, where g and τ are isogenies and g is separable (and $m = 0$ if $\mathrm{char}(L) = 0$). It suffices to prove the result for g and τ^m separately. For g, note that there exists some $b \in A$ such that $\varphi(b)$ annihilates $\ker(g)$. This implies that $\varphi(b) = f'g$ for some $f' \in L[\tau]$. This f' is the desired isogeny $X' \to X$: indeed, for any $a \in A$ we have

$$\varphi(a)f'g = \varphi(a)\varphi(b) = \varphi(b)\varphi(a) = f'g\varphi(a) = f'\varphi'(a)g$$

and hence $\varphi(a)f' = f'\varphi'(a)$.

For the purely inseparable case, choose any $b \in A$ that vanishes to order at least m at v. Then $\varphi(b) = f'\tau^m$ for some $f' \in L[\tau]$, and the same proof gives that f' is the desired isogeny. □

Let us now prove that given two elliptic modules (E, φ) and (E', φ') over L, the space of isogenies $\mathrm{Hom}(E, E')$ is a projective A-module. (To be added..)

Email address: mikayelm@mit.edu