Journal of Number Theory 165 (2016) 1–14

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Drinfeld modular polynomials in higher rank II: Kronecker congruences

Florian Breuer [a,*,1], Hans-Georg Rück [b]

[a] Department of Mathematical Sciences, University of Stellenbosch, Stellenbosch, 7600, South Africa
[b] Institut für Mathematik, Universität Kassel, Kassel, 34132, Germany

ARTICLE INFO

Article history:
Received 19 March 2013
Received in revised form 6 January 2016
Accepted 15 January 2016
Available online 3 March 2016
Communicated by David Goss

Keywords:
Drinfeld modules
Modular polynomials
Isogenies
Isomorphism invariants

ABSTRACT

This is a sequel to the paper [4], in which we introduced Drinfeld modular polynomials of higher rank, using an analytic construction. These polynomials relate the isomorphism invariants of Drinfeld $\mathbb{F}_q[T]$-modules of rank $r \geq 2$ linked by isogenies of a specified type. In the current paper, we give an algebraic construction of greater generality, and prove a generalization of the Kronecker congruences relations, which describe what happens when modular polynomials associated to P-isogenies are reduced modulo a prime P. We also correct an error in [4].

1. Isomorphism invariants

Denote by $\mathbb{F}_q$ the finite field of q elements, where q is a power of the prime p. Let $A = \mathbb{F}_q[T]$ and let $r \geq 2$ be a positive integer. Let $g_1, \ldots, g_{r-1}$ be algebraically independent over $k = \mathbb{F}_q(T)$, and let $B = A[g_1, \ldots, g_{r-1}] = \mathbb{F}_q[T, g_1, \ldots, g_{r-1}]$. Denote by $\tau : x \mapsto x^q$

* Corresponding author.
E-mail addresses: fbreuer@sun.ac.za (F. Breuer), rueck@mathematik.uni-kassel.de (H.-G. Rück).
[1] Supported by an Alexander von Humboldt Fellowship for Experienced Researchers, and by the NRF grants BS2008100900027 and IFRR96241.

http://dx.doi.org/10.1016/j.jnt.2016.01.001
0022-314X/

the q-Frobenius, and for any ring R of characteristic p we denote by $R\{\tau\}$ the ring of twisted polynomials in τ with coefficients in R, subject to the commutation relations $\tau a = a^q \tau$ for all $a \in R$.

Let $\varphi : A \to B\{\tau\}$ be the Drinfeld A-module of rank r of generic characteristic determined by

$$\varphi_T = T + g_1\tau + \cdots + g_{r-1}\tau^{r-1} + \tau^r.$$

We think of φ as the *monic generic Drinfeld A-module of rank r*. A general reference for Drinfeld modules is [5, §4].

The group $\mathbb{F}_{q^r}^*$ acts on $B \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$ via

$$\lambda * (g_k \otimes 1) = g_k \otimes \lambda^{q^k-1}, \qquad k = 1, 2, \ldots, r-1,$$

and we denote by

$$C := (B \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r})^{\mathbb{F}_{q^r}^*} \cap B$$

the subring of invariants with coefficients in $\mathbb{F}_q$. Equivalently, C consists of those polynomials in B whose monomials are of the form $f(T)g_1^{e_1}g_2^{e_2}\cdots g_{r-1}^{e_{r-1}}$ satisfying $f(T) \in A = \mathbb{F}_q[T]$ and

$$\sum_{k=1}^{r-1} e_k(q^k - 1) \equiv 0 \bmod q^r - 1.$$

Recall that an *A-field* is a field L together with a ring homomorphism $\gamma : A \to L$.

Proposition 1.1. *For every algebraically closed A-field L, there is a canonical bijection between the set of isomorphism classes of rank r Drinfeld A-modules over L, and ring homomorphisms $m : C \to L$ satisfying $m|_A = \gamma$.*

Proof. Let $\psi : A \to L\{\tau\}$ be a rank r Drinfeld A-module over the algebraically closed A-field L, then up to isomorphism we may assume that it is monic, i.e. that

$$\psi_T = \gamma(T) + a_1\tau + \cdots + a_{r-1}\tau^{r-1} + \tau^r, \qquad a_i \in L.$$

We associate to ψ the ring homomorphism

$$m_\psi : B \to L \quad \text{ with } m_\psi(g_i) = a_i \text{ and } m|_A = \gamma.$$

Let $\iota : C \hookrightarrow B$ be the inclusion, then the homomorphism

$$m_\psi \circ \iota : C \to L$$

is invariant under isomorphisms of the Drinfeld module ψ.

Conversely, let $m : C \to L$ be a ring homomorphism with $m|_A = \gamma$. For each $i = 1, 2, \dots, r-1$ we have $g_i^{q^r-1} \in C$, therefore we can extend m to B by defining $m(g_i)$ to be a chosen (q^r-1)st root of $m(g_i^{q^r-1})$ in L.

Each homomorphism $m : B \to L$ yields a Drinfeld module ψ with

$$\psi_T = \gamma(T) + m(g_1)\tau + \cdots + m(g_{r-1})\tau^{r-1} + \tau^r.$$

Now let ψ and $\tilde{\psi}$ be two Drinfeld modules such that $m_\psi \circ \iota = m_{\tilde{\psi}} \circ \iota$. We have to show that ψ and $\tilde{\psi}$ are isomorphic over L.

The group $\mathbb{F}_{q^r}^*$ acts on $B \otimes_{\mathbb{F}_q} L = (B \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}) \otimes_{\mathbb{F}_{q^r}} L$ by $\lambda * (g_i \otimes l) = g_i \otimes \lambda^{q^i-1} l$ and m_ψ extends to $m_\psi : B \otimes_{\mathbb{F}_q} L \to L$ as

$$m_\psi(g_i \otimes l) = m_\psi(g_i) l.$$

Similarly, $(m_\psi \circ \iota)$ extends to $(m_\psi \circ \iota) : C \otimes_{\mathbb{F}_q} L \to L$.

Suppose that ψ and $\tilde{\psi}$ are not isomorphic, then for each $\lambda \in \mathbb{F}_{q^r}^*$, there is a $g_\lambda \in \{g_1, g_2 \dots, g_{r-1}\}$ for which $m_\psi(\lambda * (g_\lambda \otimes 1)) \neq m_{\tilde{\psi}}(g_\lambda \otimes 1)$. We consider the element $f \in B \otimes_{\mathbb{F}_q} L$ defined by

$$f = 1 \otimes 1 - \prod_{\lambda \in \mathbb{F}_{q^r}^*} \frac{g_\lambda \otimes 1 - 1 \otimes m_\psi(\lambda * (g_\lambda \otimes 1))}{1 \otimes \left(m_{\tilde{\psi}}(g_\lambda \otimes 1) - m_\psi(\lambda * (g_\lambda \otimes 1))\right)}.$$

We evaluate

$$m_{\tilde{\psi}}(f) = 0 \text{ and } m_\psi(\mu * f) = 1 \text{ for each } \mu \in \mathbb{F}_{q^r}^*.$$

This yields

$$1 = m_\psi\Big(\prod_{\mu \in \mathbb{F}_{q^r}^*} (\mu * f)\Big) = (m_\psi \circ \iota)\Big(\prod_{\mu \in \mathbb{F}_{q^r}^*} (\mu * f)\Big) = (m_{\tilde{\psi}} \circ \iota)\Big(\prod_{\mu \in \mathbb{F}_{q^r}^*} (\mu * f)\Big) = 0,$$

a contradiction, which proves the proposition. In the last displayed equation, we have used the fact that $(C \otimes_{\mathbb{F}_q} L) = (B \otimes_{\mathbb{F}_q} L)^{\mathbb{F}_{q^r}^*}$, which follows from the characterization of allowed monomials of the elements of C. $\square$

Let ψ be a rank r Drinfeld A-module over the A-field L given by

$$\psi_T = \gamma(T) + a_1\tau + \cdots + a_r\tau^r, \quad a_1, a_2, \dots, a_r \in L \text{ and } a_r \neq 0.$$

Denote by $\bar{L}$ the algebraic closure of L and let $\delta \in \bar{L}$ be a (q^r-1)st root of a_r. Then ψ is isomorphic (over $\bar{L}$) to $\psi' := \delta\psi\delta^{-1}$, given by

$$\psi'_T = \gamma(T) + a'_1\tau + \cdots + a'_{r-1}\tau^{r-1} + \tau^r, \quad a'_k = \delta^{1-q^k} a_k \text{ for } k = 1, 2, \dots r-1.$$

Let $J = \sum_{i=1}^{n} f_i(T) g_1^{e_{i,1}} g_2^{e_{i,2}} \cdots g_{r-1}^{e_{i,r-1}} \in C$ be an invariant and set

$$\begin{aligned} J(\psi) &:= \sum_{i=1}^{n} \gamma\big(f_i(T)\big)(a_1')^{e_{i,1}}(a_2')^{e_{i,2}} \cdots (a_{r-1}')^{e_{i,r-1}} \\ &= \sum_{i=1}^{n} \gamma\big(f_i(T)\big) a_1^{e_{i,1}} a_2^{e_{i,2}} \cdots a_{r-1}^{e_{i,r-1}} \delta^{\sum_{i=1}^{n} \sum_{k=1}^{r-1} e_{i,k}(1-q^k)} \\ &= \sum_{i=1}^{n} \gamma\big(f_i(T)\big) a_1^{e_{i,1}} a_2^{e_{i,2}} \cdots a_{r-1}^{e_{i,r-1}} a_r^{-\sum_{i=1}^{n} \frac{1}{q^r-1} \sum_{k=1}^{r-1} e_{i,k}(q^k-1)} \in L. \end{aligned}$$

Corollary 1.2. *Let ψ and $\tilde{\psi}$ be two rank r Drinfeld A-modules over the A-field L. Then ψ and $\tilde{\psi}$ are isomorphic over the algebraic closure $\bar{L}$ if and only if $J(\psi) = J(\tilde{\psi})$ for all $J \in C$.*

Proof. Let $m_\psi : C \to \bar{L}$ be the homomorphism associated to the isomorphism class of ψ by Proposition 1.1. Then $m_\psi(J) = J(\psi)$ for all $J \in C$ and the result follows. $\square$

Remark 1.3. In fancier language, Proposition 1.1 states that Spec(C) over Spec(A) is the coarse moduli scheme parametrizing isomorphism classes of rank r Drinfeld A-modules over algebraically closed A-fields. This was first shown by I.Y. Potemine in [6].

If $r = 2$, then in fact $C = A[j]$, where $j = g_1^{q+1} = g^{q+1}/\Delta$ is the usual j-invariant of $\psi_T = \gamma(T) + g\tau + \Delta\tau^2$.

In general, the ring C is a finitely generated A-algebra, and an explicit set of generators is constructed in [6]. This means that one only needs a finite set of invariants in order to determine whether or not any two Drinfeld modules are isomorphic. For a given finite set of Drinfeld modules of generic characteristic, however, one can find a single invariant to distinguish between them.

Proposition 1.4. *Let S be a finite set of pairwise non-isomorphic rank r Drinfeld A-modules of generic characteristic. Then there exists $J \in C$ such that J* distinguishes *S, i.e. $J(\varphi_1) \neq J(\varphi_2)$ for all $\varphi_1 \neq \varphi_2 \in S$.*

Proof. We use induction on $n := |S|$. The result is clearly true for $n \leq 2$. Let $n \geq 3$, and suppose that the statement is true for sets of cardinality $n-1$. Pick $\varphi_1 \in S$ and let $S_1 := S \smallsetminus \{\varphi_1\}$. By the induction hypothesis, there exists $J_1 \in C$ which distinguishes S_1. If J_1 distinguishes S then we're done. If not, then there exists $\varphi_2 \in S$ such that $J_1(\varphi_1) = J_1(\varphi_2)$, and moreover $\{\varphi_1, \varphi_2\}$ is the only pair in S on which J_1 takes the same value.

Pick $J_2 \in C$ which distinguishes $\{\varphi_1, \varphi_2\}$, and consider $J_a := J_1 + aJ_2$ for all $a \in A$. If J_a distinguishes S for some $a \in A$, then we're done. If not, then there exists a pair $\psi_1, \psi_2 \in S$ for which $J_a(\psi_1) = J_a(\psi_2)$ for at least two distinct values of $a \in A$. From this, we easily deduce that $J_1(\psi_1) = J_1(\psi_2)$, which forces $\{\psi_1, \psi_2\} = \{\varphi_1, \varphi_2\}$, and $J_2(\psi_1) = J_2(\psi_2)$, which is a contradiction. $\square$

Remark 1.5. The conclusion of Proposition 1.4 can fail in special characteristic. For example, let $L = \mathbb{F}_2$ of characteristic $\ker\gamma = T\mathbb{F}_2[T]$ and $r = 3$. Then the three Drinfeld $\mathbb{F}_2[T]$-modules defined over L by

$$\psi_T^1 = \tau^3, \qquad \psi_T^2 = \tau + \tau^3, \qquad \psi_T^3 = \tau^2 + \tau^3$$

are pair-wise non-isomorphic, as witnessed by the invariants $g_1^7,\ g_2^7 \in C$, but no single $J \in C$ can distinguish between all three since $J(\psi^i) \in \mathbb{F}_2$ for every $J \in C$ and $i = 1, 2, 3$.

2. Isogenies and modular polynomials

Let $N \in A$ be monic, then φ_N applied to a variable X defines an $\mathbb{F}_q$-linear polynomial $\varphi_N(X) \in B[X]$ which is monic and separable over B of degree $q^{r \deg N}$. Let $K = \mathrm{Quot}(B) = \mathbb{F}_q(T, g_1, \ldots, g_{r-1})$, denote by K_N the splitting field of $\varphi_N(X)$ over K, and let R_N be the integral closure of B in K_N. Then the set $\varphi[N] \subset R_N$ of roots of $\varphi_N(X)$ is an A-module isomorphic to $(A/NA)^r$.

The Galois group $\mathrm{Gal}(K_N/K)$ respects this A-module structure, and in fact it is shown in [3] that

$$\mathrm{Gal}(K_N/K) \cong \mathrm{Aut}(\varphi[N]) \cong \mathrm{GL}_r(A/NA).$$

Let f be an isogeny from φ to another Drinfeld module $\varphi^{(f)}$, defined over an extension of K. This means that

$$f\varphi_T = \varphi_T^{(f)} f. \tag{1}$$

Write $f = f_0 + f_1\tau + \cdots + f_d\tau^d$. Replacing f by $f_d^{-1} f$ gives

$$(f_d^{-1} f)\varphi_T = (f_d^{-1}\varphi_T^{(f)} f_d)\,(f_d^{-1} f),$$

so if we replace $\varphi^{(f)}$ by an isomorphic Drinfeld module, we may assume that $f_d = 1$, i.e. f is monic. In this case, there exists a monic $N \in A$ such that

$$\ker f \subset \varphi[N],$$

and so $f \in R_N\{\tau\}$. Now comparing the coefficients of the highest powers of τ in (1) shows that $\varphi_T^{(f)} \in R_N\{\tau\}$ is also monic. For any invariant $J \in C$ we find that $J(\varphi^{(f)}) \in R_N$.

Definition 2.1. Any isogeny f of φ satisfying $\ker f \subset \varphi[N]$ is called an N*-isogeny*.

Denote by I_N the set of all monic N-isogenies $f \in R_N\{\tau\}$, as above. Since any such f is determined by its kernel, the set I_N is finite.

Definition 2.2. Let $J \in C$ be an invariant. We call

$$\Phi_{J,N}(X) := \prod_{f \in I_N} \left(X - J(\varphi^{(f)})\right) \in R_N[X]$$

the *full modular polynomial of level N associated to J.*

Definition 2.3. Let $H \subset \varphi[N] \cong (A/NA)^r$ be an A-submodule. Any isogeny $f \in I_N$ for which $\ker f$ is an element of the $\mathrm{GL}_r(A/NA)$ orbit of H is called an isogeny of *type H*.

Let $J \in C$ be an invariant. Then we call

$$\Phi_{J,H}(X) := \prod_{f \in I_N \text{ of type } H} \left(X - J(\varphi^{(f)})\right) \in R_N[X]$$

the *modular polynomial of type H associated to J.*

Proposition 2.4. *Let $H \subset \varphi[N]$ be an A-submodule, and $J \in C$. Then $\Phi_{J,H}(X) \in C[X]$. Furthermore, if $J \in C$ distinguishes the Drinfeld modules $\{\varphi^{(f)} \mid f$ of type $H\}$, then $\Phi_{J,H}(X)$ is irreducible over K.*

Proof. By construction, $\Phi_{J,H}(X) \in R_N[X]$ and $\mathrm{Gal}(K_N/K)$ permutes the roots of $\Phi_{J,H}(X)$, so its coefficients lie in $R_N \cap K = B$.

We next show that $\Phi_{J,H}(X) \in C[X]$. Let $\lambda \in \mathbb{F}_{q^r}^*$ and consider the isomorphic Drinfeld module $\psi := \lambda^{-1}\varphi\lambda$, so

$$\psi_T = T + a_1\tau + \cdots + a_{r-1}\tau^{r-1} + \tau^r,$$

with each $a_i = \lambda^{q^i-1}g_i \in \mathbb{F}_{q^r}[T, g_1, \ldots, g_{r-1}] \cong B \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$.

We note that $\psi[N] = \lambda^{-1}(\varphi[N])$, and so every N-isogeny $f : \varphi \to \varphi^{(f)}$ of type $H \subset \varphi[N]$ corresponds to an N-isogeny $\lambda^{-1}f\lambda : \psi \to \psi^{(\lambda^{-1}f\lambda)} = \lambda^{-1}\varphi^{(f)}\lambda$ of type $\lambda^{-1}H \subset \psi[N]$.

Thus, if we specialize the coefficients of $\Phi_{J,H}(X)$ via $g_i \mapsto a_i = \lambda^{q^i-1}g_i$, we obtain the monic polynomial $\Phi_{J(\psi),H}(X)$ whose roots are precisely the $J(\psi^{(\lambda^{-1}f\lambda)})$ for $f \in I_N$ of type H. But $J(\psi^{(\lambda^{-1}f\lambda)}) = J(\lambda^{-1}\varphi^{(f)}\lambda) = J(\varphi^{(f)})$, so $\Phi_{J(\psi),H}(X) = \Phi_{J,H}(X)$ and we have shown that the coefficients of $\Phi_{J,H}(X)$ are $\mathbb{F}_{q^r}^*$-invariant in $B \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$. Thus $\Phi_{J,H}(X) \in C[X]$.

Lastly, the condition on J ensures a one-to-one correspondence between the roots of $\Phi_{J,H}(X)$ and $\{\varphi^{(f)} \mid f$ of type $H\}$. Since $\mathrm{Gal}(K_N/K) \cong \mathrm{GL}_r(A/NA)$ acts transitively on these roots, $\Phi_{J,H}(X)$ is irreducible over K. $\square$

Corollary 2.5. *The full modular polynomial satisfies $\Phi_{J,N}(X) \in C[X]$, and if J distinguishes the Drinfeld modules $\{\varphi^{(f)} \mid f \in I_N\}$, then the K-irreducible factors of $\Phi_{J,N}(X)$ are precisely the $\Phi_{J,H}(X)$ for various types $H \subset \varphi[N]$.* □

When $r = 2$, then $C = A[j]$ and $\Phi_{j,(A/NA)}(X) = \Phi_N(j, X) \in A[j, X]$ is the usual Drinfeld modular polynomial constructed in [2].

Let ψ be a rank r Drinfeld A-module defined over an A-field L. Then the coefficients of $\Phi_{J,H}(X) \in C[X]$ can be applied to ψ (equivalently, m_ψ from Proposition 1.1 can be applied to each coefficient), resulting in a polynomial

$$\Phi_{J(\psi),H}(X) \in L[X],$$

whose roots are precisely the $J(\psi^{(f)})$ for N-isogenies $f : \psi \to \psi^{(f)}$ of type H, which we will prove below. If N is not prime to the characteristic $\ker(\gamma)$ of ψ, then we need to make the notion of "N-isogeny of type H" more precise.

For our purposes we define a level-N structure on ψ to be a surjective A-module homomorphism

$$\mu : \varphi[N] \longrightarrow \psi[N] \subset \bar{L}.$$

When N is prime to the characteristic $\ker(\gamma)$ of ψ, then μ is an isomorphism. If μ and μ' are two level-N structures on ψ, then there is a $\sigma \in \mathrm{GL}_r(A/NA)$ such that $\mu' = \mu \circ \sigma$.

Let $H \subset \varphi[N]$ be an A-submodule. Then an isogeny $f : \psi \to \psi^{(f)}$ is said to be of type H if $f(X) = \prod_{h \in H'}(X - \mu(h))$, where $H' \subset \varphi[N]$ is an element of the $\mathrm{GL}_r(A/NA)$-orbit of H. The set of isogenies of ψ of type H is independent of the chosen level structure μ. We have

Proposition 2.6. *Let ψ be a rank r Drinfeld A-module over the A-field L, let $J \in C$ be an invariant and $H \subset \varphi[N]$ an A-submodule. Then*

$$\Phi_{J(\psi),H}(X) = \prod_{f \text{ of type } H} \left(X - J(\psi^{(f)})\right) \in L[X].$$

Proof. We have

$$\varphi_T(X) = \prod_{u \in \varphi[T]} (X - u) = TX + g_1 X^q + \cdots + g_{r-1} X^{q^{r-1}} + X^{q^r},$$

so the $g_i \in \mathbb{F}_q\left[u \ : \ u \in \varphi[T]\right]$ are polynomials over $\mathbb{F}_q$ in the u's. Moreover, these polynomials are invariant under the $\mathrm{GL}_r(A/TA)$-action on $\varphi[T]$.

Next, let $f : \varphi \to \varphi^{(f)}$ be an isogeny of type H, then for a suitable $H' \subset \varphi[N]$ we have

$$f(X) = \prod_{h\in H'} (X-h) = f_0 X + f_1 X^q + \cdots + f_{d-1} X^{q^{d-1}} + X^{q^d},$$

where $d = \dim_{\mathbb{F}_q}(H)$. Again, we see that the $f_i \in \mathbb{F}_q[h \ : \ h \in H']$ are polynomials over $\mathbb{F}_q$ in the h's.

Write $\varphi^{(f)} = T + g_1'\tau + \cdots + g_{r-1}'\tau^{r-1} + \tau^r$, then comparing coefficients of $\tau^{dr-1}, \tau^{dr-2}, \ldots, \tau^{dr-r+1}$ in $f \cdot \varphi_T = \varphi_T^{(f)} \cdot f$, we obtain

$$g_i' \in \mathbb{F}_q[T, g_1, \ldots, g_{r-1}, f_1, \ldots, f_{d-1}] \subset \mathbb{F}_q[u, h \ : \ u \in \varphi[T], \ h \in H'].$$

As a result

$$J(\varphi^{(f)}) \in \mathbb{F}_q[u, h \ : \ u \in \varphi[T], \ h \in H'],$$

but $J \in C \subset \mathbb{F}_q[T, g_1, \ldots, g_{r-1}]$, so in fact $J(\varphi^{(f)}) \in \mathbb{F}_q\big[u \ : \ u \in \varphi[T]\big]$.

Now, replacing ψ by an isomorphic Drinfeld module over $\bar{L}$ if necessary, we may assume that

$$\psi_T = \gamma(T) + a_1\tau + \cdots + a_{r-1}\tau^{r-1} + \tau^r, \quad a_1, \ldots, a_{r-1} \in \bar{L},$$

is monic. Let $M = \mathrm{lcm}(T, N)$ and let $\mu : \varphi[M] \to \psi[M]$ be a level-M structure on ψ. By the same arguments as above, replacing each u by $\mu(u)$ and each h by $\mu(h)$, we find that each

$$J(\psi^{(f)}) \in \mathbb{F}_q\big[\mu(u) \ : \ u \in \varphi[T]\big]$$

is the same polynomial as $J(\varphi^{(f)})$, but with each u replaced by $\mu(u)$.

Applying the map μ to the polynomials $g_i \in \mathbb{F}_q\big[u \ : \ u \in \varphi[T]\big]$, each g_i is mapped to a_i, hence μ coincides there with the homomorphism $m_\psi : C \to \bar{L}$ from Proposition 1.1. Thus, for each isogeny f of type H, we obtain

$$m_\psi\big(J(\varphi^{(f)})\big) = J(\psi^{(f)}),$$

which completes the proof. $\square$

3. Correction to [4]

In [4] we gave an analytic construction of modular polynomials of type $(A/NA)^{r-1}$. These polynomials also classify *incoming* isogenies $\varphi' \to \varphi$ with kernels isomorphic to A/NA, whereas the point of view of the present article is to classify modular polynomials by the kernels of the dual, *outgoing* isogenies $f : \varphi \to \varphi'$, which explains the shift in terminology from type A/NA to type $(A/NA)^{r-1}$.

Theorem 1.1 of [4] claims that the polynomials $\Phi_{J,(A/NA)^{r-1}}(X)$ are irreducible, but this is only true if $J \in C$ distinguishes the set of Drinfeld modules $\{\varphi^{(f)} \mid f$ of type $(A/NA)^{r-1}\}$, i.e. when $\Phi_{J,(A/NA)^{r-1}}(X)$ has distinct roots. Such invariants $J \in C$ always exist, by Proposition 1.4.

4. Reduction mod P and Kronecker congruence relations

In this section, we let $N = P \in A$ be a monic prime, and we study the reduction of modular polynomials modulo P. When we reduce polynomials in $R_P[X]$, then we are actually reducing modulo a chosen prime of R_P extending PB (remember that R_P is integral over B), but we will still write mod P for ease of notation.

Define $\mathbb{F}_P := A/PA$. We start with the following basic result.

Proposition 4.1. *We have*

$$\varphi_P \equiv \tilde{\varphi}_P \cdot \tau^{\deg(P)} \bmod P\,,$$

where $\tilde{\varphi}_P \in (B \otimes_A \mathbb{F}_P)\{\tau\}$ is not divisible by τ.

In other words, φ has ordinary reduction at every prime P.

We will give two proofs of this result, starting with a conceptual proof.

Proof. Denote by $\bar{\varphi} : A \to (B \otimes_A \mathbb{F}_P)\{\tau\}$ the reduction of φ modulo P. We have $\bar{\varphi}[P] \cong (A/PA)^{r-h}$, where h is the height of $\bar{\varphi}$ (see [5, §4.5]). The linear term of φ_P is P, so $\bar{\varphi}_P$ is divisible by τ and thus $h \geq 1$. We will show that $h = 1$ by constructing a specialization of φ with ordinary reduction at a prime above P.

Recall that $k = \mathbb{F}_q(T)$ and let F/k be a separable extension of degree r which has only one place above the place of k with uniformizer $1/T$ (i.e. F/k is *purely imaginary*) and in which P splits completely (such a field exists, by [1, Chapter X, Theorem 6]). Denote by R the integral closure of A in F, and let ψ be a rank 1 Drinfeld R-module, which is automatically a rank r Drinfeld A-module with complex multiplication by R (for example, let ψ be the Drinfeld module corresponding to the lattice R in the algebraic closure of $\mathbb{F}_q((\frac{1}{T})))$. Let $PR = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ be the factorization of PR in R. Let L/F be a finite extension over which ψ is defined, let $\mathfrak{P}_1$ be a place of L above $\mathfrak{p}_1$, and denote by $\mathcal{O}_{\mathfrak{P}_1}$ the valuation ring of $\mathfrak{P}_1$. Since all rank 1 Drinfeld modules have potential good reduction by [5, Cor. 4.10.4], we may write

$$\psi_T = T + a_1\tau + a_2\tau^2 + \cdots + a_r\tau^r, \quad \text{with} \quad a_1, \ldots, a_{r-1} \in \mathcal{O}_{\mathfrak{P}_1},\ a_r \in \mathcal{O}_{\mathfrak{P}_1}^*.$$

After possibly replacing L by a finite extension and ψ by an isomorphic Drinfeld module, we may assume furthermore that $a_r = 1$, so that ψ is the image of φ under the specialization $g_i \mapsto a_i,\ i = 1, 2, \ldots, r-1$.

Denote by $\bar{\psi}$ the reduction of ψ modulo $\mathfrak{P}_1$, then the P-torsion module of $\bar{\psi}$ is

$$\begin{aligned} \bar{\psi}[P] = \bar{\psi}[PR] \;&\cong\; \bar{\psi}[\mathfrak{p}_1] \times \bar{\psi}[\mathfrak{p}_2] \times \cdots \times \bar{\psi}[\mathfrak{p}_r] \\ &\cong \{0\} \times (A/PA)^{r-1}, \end{aligned}$$

as required. □

We also provide an elementary proof of Proposition 4.1.

Proof. We specialize φ to ψ, where $\psi_T = T + g_1\tau + \tau^r$, and show that ψ has ordinary reduction at P.

For each positive integer i, we study the 3^i monomials $m = m(T, g_1, \tau)$ in $(\psi_T)^i$, which are constructed from the non-commuting factors T, $g_1\tau$ and τ^r. We call m *simple* if no τ^r-factor was used in the construction of m. The monomial m can be written uniquely in the form $T^a g_1^b \tau^c$ and we set $\deg_{g_1}(m) := b$ and $\deg_\tau(m) := c$.

By induction on i, one readily shows that

$$\deg_{g_1}(m) \leq \frac{q^{\deg_\tau(m)} - 1}{q-1},$$

with equality if and only if m is simple.

Now suppose $P = \sum_{i=0}^{s} a_i T^i$, with $a_s = 1$, is our monic prime in A of degree s. We consider the coefficient $b_s(T, g_1)$ of τ^s in

$$\psi_P = \sum_{i=0}^{s} a_i (\psi_T)^i = \sum_{j=0}^{rs} b_j(T, g_1)\tau^j.$$

One of the terms of $b_s(T, g_1)$ is $g_1^{(q^s-1)/(q-1)}$, arising from the monomial $(g_1\tau)^s$ in $(\psi_T)^s$, whereas all other terms have strictly smaller degree in g_1, since they arise from non-simple monomials in $(\psi_T)^i$ with $i \leq s$. It follows that $b_s(T, g_1)$ does not vanish modulo P, and so the reduction of ψ modulo P has height 1, as required. □

Corollary 4.2. *There exists a unique monic P-isogeny f_0 of φ satisfying*

1. $f_0 \equiv \tau^{\deg P} \bmod P$*,*
2. $U_0 := \ker f \cong A/PA = \mathbb{F}_P$ *as A-modules, and*
3. $f_0\varphi = \varphi^{(f_0)} f_0$*, where*

$$\varphi_T^{(f_0)} \equiv T + g_1^{|P|}\tau + \cdots + g_{r-1}^{|P|}\tau^{r-1} + \tau^r \bmod P.$$

Proof. Let $U_0 = \ker\left(\varphi[P] \longrightarrow \bar{\varphi}[P]\right)$ denote the kernel of reduction modulo P. Then by Proposition 4.1, $U_0 \cong A/PA$, and

$$f_0(X) := \prod_{u_0 \in U_0} (X - u_0) \equiv X^{|P|} \bmod P.$$

It is now easy to verify that f_0 has all the required properties. □

Since the kernel of any P-isogeny f is an $\mathbb{F}_P$-vector space, its kernel $U := \ker f$ satisfies either $U_0 \cap U = \{0\}$, in which case we call f *ordinary*, or else $U_0 \subset U$, in which case we call f *special*. Equivalently, f is ordinary if the reduction of f modulo P is separable, and special otherwise.

Definition 4.3. Let $H \subset \varphi[P]$ be an A-submodule and $J \in C$ an invariant. We define the following factors of the modular polynomial $\Phi_{J,H}(X)$:

$$\Phi^{\mathrm{spec}}_{J,H}(X) := \prod_{f \in I_P \text{ special of type } H} \left(X - J(\varphi^{(f)})\right) \in R_P[X], \quad \text{and}$$

$$\Phi^{\mathrm{ord}}_{J,H}(X) := \prod_{f \in I_P \text{ ordinary of type } H} \left(X - J(\varphi^{(f)})\right) \in R_P[X].$$

Clearly $\Phi_{J,H}(X) = \Phi^{\mathrm{spec}}_{J,H}(X) \cdot \Phi^{\mathrm{ord}}_{J,H}(X)$.

We are now ready to prove our main result.

Theorem 4.4 *(Kronecker Congruence Relations). Let $P \in A$ be a monic prime, $J \in C$ an invariant and $1 \leq s < r$. Then*

1. $\Phi^{\mathrm{ord}}_{J,(A/PA)^s}(X) \equiv \left(\Phi^{\mathrm{spec}}_{J,(A/PA)^{s+1}}(X^{|P|})\right)^{|P|^{s-1}} \bmod P$, *and*
2. $\Phi_{J,(A/PA)^s}(X) \equiv \Phi^{\mathrm{spec}}_{J,(A/PA)^s}(X) \cdot \left(\Phi^{\mathrm{spec}}_{J,(A/PA)^{s+1}}(X^{|P|})\right)^{|P|^{s-1}} \bmod P$.

Furthermore,

3. *The reductions of $\Phi^{\mathrm{spec}}_{J,(A/PA)^s}(X)$ and $\Phi^{\mathrm{ord}}_{J,(A/PA)^s}(X)$ modulo P lie in $(C \otimes_A \mathbb{F}_P)[X]$ for every $s = 1, \ldots, r$.*

Proof. Let $1 \leq s < r$. Let f_U and $f_{\tilde{U}}$ be two ordinary P-isogenies of type $H \cong (A/PA)^s$ with kernels U and $\tilde{U}$, respectively. We call f_U and $f_{\tilde{U}}$ *equivalent* if $U + U_0 = \tilde{U} + U_0$. This way each equivalence class contains $|P|^s$ elements, since the kernel of each isogeny in the equivalence class of f_U is obtained by adding elements of U_0 to each of the s basis vectors of U. The P-isogeny f_{U+U_0} with kernel $U + U_0$ is then special of type $(A/PA)^{s+1}$, and moreover each special isogeny of type $(A/PA)^{s+1}$ arises from an equivalence class of ordinary isogenies of type $(A/PA)^s$ in this way.

We see that

$$\begin{aligned} f_{U+U_0}(X) &= \prod_{u\in U}\prod_{u_0\in U_0}\big(X-u-u_0\big) \equiv \prod_{u\in U}(X-u)^{|P|} \equiv f_U(X)^{|P|} \\ &\equiv \tau^{\deg P}\big(f_U(X)\big) \bmod P. \end{aligned}$$

Thus, for the corresponding isogenous Drinfeld modules,

$$\begin{aligned} \varphi^{(U+U_0)}\cdot\tau^{\deg P}\cdot f_U \equiv \varphi^{(U+U_0)}\cdot f_{U+U_0} &= f_{U+U_0}\cdot\varphi \equiv \tau^{\deg P}\cdot f_U\cdot\varphi \\ &= \tau^{\deg P}\cdot\varphi^{(U)}\cdot f_U \bmod P, \end{aligned}$$

and we obtain

$$\varphi^{(U+U_0)}\cdot\tau^{\deg(P)} \equiv \tau^{\deg(P)}\cdot\varphi^{(U)} \bmod P.$$

For any invariant $J\in C$ we now have

$$J(\varphi^{(U+U_0)}) \equiv J(\varphi^{(U)})^{|P|} \bmod P.$$

If we combine these results, we calculate

$$\begin{aligned} \Big(\Phi^{\mathrm{ord}}_{J,(A/PA)^s}(X)\Big)^{|P|} &\equiv \prod_{f_U\ \text{ordinary of type}\ (A/PA)^s}\big(X^{|P|}-J(\varphi^{(U)})^{|P|}\big) \bmod P \\ &\equiv \prod_{f_{(U+U_0)}\ \text{special of type}\ (A/PA)^{s+1}}\big(X^{|P|}-J(\varphi^{(U+U_0)})\big)^{|P|^s} \bmod P \\ &\equiv \Big(\Phi^{\mathrm{spec}}_{J,(A/PA)^{s+1}}(X^{|P|})\Big)^{|P|^s} \bmod P, \end{aligned}$$

from which (1.) follows.

Next, (2.) follows from (1.) and $\Phi_{J,(A/PA)^s}(X)=\Phi^{\mathrm{spec}}_{J,(A/PA)^s}(X)\cdot\Phi^{\mathrm{ord}}_{J,(A/PA)^s}(X)$.

It remains to prove (3.). If $s=r$, then

$$\Phi_{J,(A/PA)^r}(X)=\Phi^{\mathrm{spec}}_{J,(A/PA)^r}(X)=X-J,$$

since the only isogeny of type $(A/PA)^r$ is the endomorphism φ_N, and of course

$$\Phi^{\mathrm{ord}}_{J,(A/PA)^r}(X)=1.$$

Now suppose that $\Phi^{\mathrm{spec}}_{J,(A/PA)^s}(X) \bmod P\in(C\otimes_A\mathbb{F}_P)[X]$ for some $1\le s\le r$. Since also $\Phi_{J,(A/PA)^{s-1}}(X) \bmod P\in(C\otimes_A\mathbb{F}_P)[X]$, it follows from (2.), with s replaced by $s-1$, that $\Phi^{\mathrm{spec}}_{J,(A/PA)^{s-1}}(X) \bmod P\in(C\otimes_A\mathbb{F}_P)[X]$. Indeed, if this where not the case, consider its highest coefficient not in $C\otimes_A\mathbb{F}_P$ and remember that all our polynomials are monic.

Lastly, it follows from (1.) that now also $\Phi^{\mathrm{ord}}_{J,(A/PA)^s}(X) \bmod P\in(C\otimes_A\mathbb{F}_P)[X]$. $\square$

Question 4.5. Suppose that J distinguishes the reduced Drinfeld modules $\bar{\varphi}^{(f)}$ for special isogenies $f \in I_P$. Is $\Phi^{\mathrm{spec}}_{J,(A/PA)^s}(X)$ irreducible modulo P?

5. Examples

Example 1. **s** $= 1$: In this case

$$\Phi^{\mathrm{spec}}_{J,(A/PA)}(X) = X - J(\varphi^{(f_0)}) = X - J^{|P|},$$

by Corollary 4.2, so

$$\Phi_{J,(A/PA)}(X) \equiv (X - J^{|P|}) \cdot \Phi^{\mathrm{spec}}_{J,(A/PA)^2}(X^{|P|}) \bmod P.$$

Example 2. **s** $= r-1$: We have

$$\Phi^{\mathrm{spec}}_{J,(A/PA)^r}(X) = X - J(\varphi^{(\varphi_N)}) = X - J,$$

so

$$\Phi_{J,(A/PA)^{r-1}}(X) \equiv \Phi^{\mathrm{spec}}_{J,(A/PA)^{r-1}}(X) \cdot \left(X^{|P|} - J\right)^{|P|^{r-2}} \bmod P.$$

Example 3. **r** $= 2$: This is a combination of examples 1 and 2 above, and gives the classical result (see [2]):

$$\Phi_{J,(A/PA)}(X) \equiv (X - J^{|P|}) \cdot (X^{|P|} - J) \bmod P.$$

Example 4. Now suppose that $r = 3$, $P = T$ and $A = \mathbb{F}_2[T]$, see [4]. In this case,

$$C = \frac{A[J_{07}, J_{12}, J_{41}, J_{70}]}{\langle J_{07}J_{41} - J_{12}^4, \quad J_{12}J_{70} - J_{41}^2 \rangle},$$

where $J_{ij} = g_1^i g_2^j$. In [4] we computed $\Phi_{J,(A/TA)^2}(X)$ for $J \in \{J_{07}, J_{12}, J_{41}, J_{70}\}$ (they are denoted $P_{J,T}(X)$ in that paper). Reducing these modulo T, one obtains, for example,

$$\Phi_{J_{12},(A/TA)^2}(X) \equiv \Phi^{\mathrm{spec}}_{J_{12},(A/TA)^2}(X) \cdot \left(X^2 + J_{12}\right)^2 \bmod T$$

where

$$\begin{aligned}\Phi^{\mathrm{spec}}_{J_{12},(A/TA)^2}(X) \equiv X^3 &+ (J_{07}J_{12} + J_{12}^3 + J_{70})X^2 + (J_{07}J_{41} + J_{12}J_{41}J_{70} + J_{41} + J_{70}^2)X \\ &+ (J_{07}J_{12}J_{41} + J_{12}^2 J_{70} + J_{12}J_{70}^2 + J_{70}^3 + J_{70}) \bmod T.\end{aligned}$$

A similar computation, carried out with the help of Herinniaina Razafinjatovo, confirms that

$$\Phi_{J_{12},(A/TA)}(X) \equiv (X + J_{12}^2) \cdot \Phi^{\mathrm{spec}}_{J_{12},(A/TA)^2}(X^2) \bmod T,$$

with $\Phi^{\mathrm{sep}}_{J_{12},(A/TA)^2}(X)$ as above.

References

[1] E. Artin, J. Tate, Class Field Theory, AMS Chelsea, 2008.
[2] S. Bae, On the modular equation for Drinfeld modules of rank 2, J. Number Theory 42 (1992) 123–133.
[3] F. Breuer, Explicit Drinfeld moduli schemes and Abhyankar's generalized iteration conjecture, J. Number Theory 160 (2016) 432–450.
[4] F. Breuer, H.-G. Rück, Drinfeld modular polynomials in higher rank, J. Number Theory 129 (2009) 59–83.
[5] D. Goss, Basic Structures in Function Field Arithmetic, Springer-Verlag, 1996.
[6] I.Y. Potemine, Minimal terminal $\mathbb{Q}$-factorial models of Drinfeld coarse moduli schemes, Math. Phys. Anal. Geom. 1 (1998) 171–191.