Running head: Zeros of Eisenstein series April 2, 1998
Math. Subj. Class. (1991): 11G09, 11F03

Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields

by Gunther Cornelissen

Introduction

In the ample theory of classical modular forms, little attention seems to have been payed to their zeros. As is well known, the (suitably counted) number of zeros of a modular form for a congruence subgroup of $SL(2, \mathbf{Z})$ on the corresponding modular curve can be expressed in solely geometric terms, *e.g.*, the weight multiplied by a normalized hyperbolic volume of the corresponding modular curve ([19], 2.16 & 2.20).

In a different vein (following prior work of Wohlfahrt, R.A. Rankin and A.O.L. Atkin) F.K.C. Rankin and Swinnerton-Dyer [16] have used methods of classical analysis to show that zeros of Eisenstein series for $SL(2, \mathbf{Z})$ in the fundamental domain are located on the complex unit circle. R.A. Rankin [17] has subsequently generalized the result.

Now assume that $f(z)$ is a holomorphic modular form for a congruence group Γ of level N in $SL(2, \mathbf{Z})$, and that it can be defined over a finite extension $L/\mathbf{Q}$ of the rationals. By this we mean that f admits Fourier expansions in $L((e^{2\pi iz/N}))$. Assume also that L is big enough for the modular curve X_Γ to be uniformized by modular functions defined over L. From these two assumptions it follows that the points in the support of the divisor of f are defined over a finite extension of L. Hence also the j-invariants of the zeros of f, *i.e.*, the images of the zeros under the (L-rational) projection $X_\Gamma \to X(1)$, are algebraic numbers. Then a famous corollary of the Gelfond-Schneider theorem implies that *zeros in the upper half plane of any modular form defined over a finite extension of* $\mathbf{Q}$, *are either transcendental over* $\mathbf{Q}$, *or points of complex multiplication.*

In order to pursue a meaningful *algebraic* study of the zeros of f, one is led to focus on the field extension generated by the points in the support of the divisor of f, denoted by $L(\mathrm{div}(f))/L$.

Example. Let

$$E_l(z) = 1 - \frac{2}{B_l} \sum_{n \geq 1} \sum_{d|n} d^{l-1} e^{2\pi inz},$$

be the Eisenstein series of weight $l > 2$ for $SL(2, \mathbf{Z})$, normalized in such a way that it is defined over $\mathbf{Q}$ (where B_l is the l-th Bernoulli number). Set $l = 12m + 4d + 6e$ with $d \in \{0, 1, 2\}$ and $e \in \{0, 1\}$. Let $1728 \cdot \Delta = E_4^3 - E_6^2$ and $j = E_4^3/\Delta$ be the normalized discriminant Δ and the j-invariant j respectively. Then

$$E_l(z)E_4(z)^{-d}E_6(z)^{-e}\Delta(z)^{-m} = P_l(j(z))$$

for some polynomial P_l of degree m, and the divisor of E_l on the j-line $X(1)$ is given by

$$\mathrm{div}(E_l) = \frac{d}{2} \cdot 0 + \frac{e}{3} \cdot 1728 + \mathrm{div}(P_l).$$

(As usual [19], this divisor takes into account the order of the stabilizers in $SL(2, \mathbf{Z})$, and lies in $\mathrm{Pic}(X(1)) \otimes \mathbf{Q}$). One recognizes $j = 0$ and $j = 1728$ as the two elliptic points of $SL(2, \mathbf{Z})$.

E1. The theorem of Rankin and Swinnerton-Dyer is equivalent to the fact that the roots of P_l are real and belong to the interval $(0, 1728)$.

E2. Assume that $l + 1$ equals a prime number p. Weights of this form seem to be especially relevant to arithmetic due to Deligne's observation that E_{p-1} is congruent to the Hasse invariant modulo p. A bit of computation shows that for $l < 90$, $\mathrm{div}(P_l)$ is irreducible over $\mathbf{Q}$. Furthermore, one computes that

$$\mathrm{Gal}(\mathbf{Q}(\mathrm{div}(E_l))/\mathbf{Q}) = S_m$$

for the same such l. Thus, whereas the j-invariants of the zeros of E_l are algebraic, their algebraic *relations* are "without affect", *i.e.*, like the roots of the general polynomial.

E3. For the same such l, one can compute that the ramification for the extension $\mathbf{Q}(\mathrm{div}(E_l))/\mathbf{Q}$ is concentrated in the primes of degree less than $(p + 1)/2$. By this we mean that a high power of such primes always occurs in the discriminant of P_l (sometimes with the exception of the prime 11). Some larger primes might occur. □

The aim of this work is to prove that the situation of the example persists for an infinity of different weights, *albeit* in the corresponding theory of modular forms for rational function fields (Eisenstein series for GL_2 over a polynomial ring over a finite field acting on the Drinfeld upper half plane). We will also indicate how the analogue of Rankin's and Swinnerton-Dyer's theorem fits into this algebraic way of thinking. The main results will be stated after introducing some notations in the next section.

One of the reasons for having a closer look at *zeros* of modular forms seems to be the following qualitative observation. Assume f is a modular form defined over a number field L with ring of integers $\mathcal{O}$ and assume that f is congruent modulo some prime $\mathfrak{B}$ of $\mathcal{O}$ to an arithmetical function H whose zeros z in the upper half plane are important (L-functions, invariants of elliptic curves). Assume that $f(z) \in \mathcal{O}$. Then a (hopefully meaningful) inequality results as follows:

$$H(z) = 0 \Rightarrow f(z) = 0 \text{ or } |N_{\mathbf{Q}}^L f(z)| \geq |N_{\mathbf{Q}}^L \mathfrak{B}|.$$

The Γ-orbits of the zeros z of f form a finite set of "exceptional" values, and for all other values the inequality holds.

This somewhat vague principle can be applied in our situation, as we consider weights corresponding to the case where Deligne's congruence is valid: the modular form "Eisenstein series" is congruent to the arithmetical object "Hasse invariant". This also means that there will be an intimate connection to supersingularity and hence quadratic class numbers (or equivalently, type numbers of quaternion algebras). Indeed, on the way we will encounter a class number problem for certain hyperelliptic function fields, and finally we will be able to present an application to supersingular reduction of Drinfeld modules in the aforementioned sense: if a j-invariant j is supersingular modulo some prime $\mathfrak{B}$, then either it belongs to a finite list of $\mathfrak{B}$-exceptions (corresponding to the zeros), or an inequality between the degrees of $\mathfrak{B}$ and j results. Actually, the number of such $\mathfrak{B}$ of a restricted degree $\leq k$ is bounded in terms of j and k for non-exceptional j. The technical result is again stated in the next section.

I expect that most of our results obtained in the setting of a rational function field should carry through for classical Eisenstein series on $SL(2, \mathbf{Z})$ too, but I have not carried out such a programme.

1. Notations and statements

We refer to [8], [14], [10], [13] for details. Let q be a power of an *odd* prime p and $A = \mathbf{F}_q[T]$ the polynomial ring over the finite field $\mathbf{F}_q$ of q elements. Let K be the quotient field of A, and $|\cdot|$ the absolute value on K given by $|q| = q^{\deg a}$ for $a \in A$. Let K_∞ and C be respectively the completion of K and the completion of an algebraic closure of K_∞. The space $\Omega := C - K_\infty$ is called *Drinfeld's upper half space*, and carries a structure as a rigid analytic space, on which the group $GL(2, A)$ acts through fractional transformations. With respect to this action and this notion of analyticity, the function

$$E_l(z) : \Omega \to C : z \mapsto \sum_{(0,0)\neq(a,b)\in A^2} (\frac{1}{az+b})^l$$

turns out to be a modular form of weight l. It is called the *Eisenstein series* of weight l, and it is non-trivial only if $q-1$ divides l. We will set $\langle i \rangle = T^{q^i} - T$ for any natural number i. The symbol $\langle i \rangle$ equals the product of all irreducibles polynomials in A of degree dividing i. Let χ be the characteristic function of the odd integers, *i.e.* $\chi(2\mathbf{Z}+1) = 1, \chi(2\mathbf{Z}) = 0$. Define two modular forms g and Δ of respective weights $q-1$ and q^2-1 by

$$g = \langle 1 \rangle E_{q-1}, \quad \Delta = \langle 1 \rangle E_{q-1}^{q+1} - \langle 2 \rangle E_{q^2-1}.$$

The *j-invariant* $j = g^{q+1}/\Delta$ induces an isomorphism of rigid analytic spaces j-line $= GL(2, A)\backslash\Omega \to C$. Note that we have not normalized E_l, j etc. such that they are "defined over K" in the sense of the introduction. But our subsequent formulas will be written in such a form that all possible transcendentals factor out.

As will become apparent, the role played by the pair (E_{p-1}, p) for a prime p in the example above is taken over by $(E_{q^k-1}, \mathfrak{p})$ for primes $\mathfrak{p} \in A$ of degree k. We will now formulate the main theorems on the arithmetic of the divisors of these Eisenstein series.

First of all, in [5] it was proved that the divisor of the Eisenstein series E_{q^k-1} on the j-line is given by

$$\operatorname{div}(E_{q^k-1}) = \chi(k)\frac{1}{q+1} \cdot 0 + \operatorname{div}(P_k(j)),$$

where P_k is a polynomial in j. Note that $j = 0$ is the unique elliptic point for $GL(2, A)$ (i.e., whose stabilizer for the action of $GL(2, A)$ on Ω is $\mathbf{F}_{q^2}^*$ rather then the usual center $\mathbf{F}_q^*$ of $GL(2, A)$). The degree of P_k is

$$m(k) = \deg P_k = \frac{q^k - q^{\chi(k)}}{q^2 - 1}.$$

Theorem E1 ([5], compare (2.3)). *Non-zero j-invariants of zeros of Eisenstein series E_{q^k-1} (i.e., the roots of P_l) have absolute value q^q.*

Theorem E2. *For all even k, the Galois group of P_k is alternating or symmetric of degree $m(k)$. Admitting the classification of finite simple groups, if $k \equiv 0, 2$ mod 8, then there exists a constant C_k such that for all $q > C_k$, $(q, k, k-4)$ mutually coprime,*

$$\operatorname{Gal}(P_k/K) = \operatorname{Gal}(K(j(z) : E_{q^k-1}(z) = 0)/K) = S_{m(k)}.$$

Theorem E3 (Gekeler, [12]). *In the splitting field of P_k exactly all primes of degree strictly less than k are ramified.*

These theorems should be compared to the similarly numbered statements in the example from the introduction. The main task of this paper is to prove theorem E2, and then apply our "vague principle" from the introduction. Consequently the *Leitfaden* is as follows. In section two, the polynomials P_k will be introduced, a theorem of Rankin & Swinnerton-Dyer type will be derived, and properties of reductions of P_k will be related to supersingularity of Drinfeld modules, and class numbers of hyperelliptic function fields. The third paragraph will contain auxiliary results from the theory of primitive permutation groups and local Galois theory. In the fourth paragraph, a proof of the main theorem will be presented: a "big" cycle in $\operatorname{Gal}(P_k)$ is produced by consideration of certain inertia groups. Then transitivity is proved by combining a counting argument on these cycles with the analogue of Rankin's & Swinnerton-Dyer's result. A group theoretic lemma subsequently implies primitivity, and using results of Jordan-Marggraff and Wielandt, the Galois group is alternating or symmetric. In the fifth section, a link with 8-divisibility of class numbers is exploited to produce an even element in the Galois group. There, we prove the following incongruence result for class numbers of imaginary quadratic extensions of function fields:

Theorem H. *(i) Fix a non-square $e \in \mathbf{F}_q$. For a prime $\mathfrak{p}$ of A, the class number of $A[\sqrt{e\mathfrak{p}}]$ is even if and only if* $\deg \mathfrak{p}$ *is, and is divisible by 4 if and only if* $\deg \mathfrak{p}$ *is.*

(ii) Assume the classification of finite simple groups. If k is a fixed integer divisible by 8, and e as before, then there exists a constant C_k such that for all $q > C_k$ coprime with k and $k-4$, there exist two primes $\mathfrak{p}$ and $\mathfrak{p}'$ such that the class numbers of $A[\sqrt{e\mathfrak{p}}]$ and $A[\sqrt{e\mathfrak{p}'}]$ are incongruent modulo 8.

The main complication in the proof of theorem H is the fact that one has to find *irreducible* $\mathfrak{p}$ and $\mathfrak{p}'$. The proof involves genus theory, and the explicit construction of certain ambiguous classes necessitates the use of distribution results for irreducible polynomials over finite fields.

As the class number of $A[\sqrt{e\mathfrak{p}}]$ is twice the number of $\mathbf{F}_q$-rational points on the Jacobian of the normalization of the plane curve $y^2 = e\mathfrak{p}(t)$ in the (t, y)-plane, one can reinterpret theorem H in a geometric fashion.

Finally, an application to supersingular reduction of Drinfeld modules is given in section six, generalizing [6]. Assume that F is a field equipped with an A-algebra structure $i : A \to F$. Let

$$\phi : A \to \mathrm{End}(\mathbf{G}_a(F))$$

be a rank two A-Drinfeld module defined over F, *i.e.* a ring morphism from A to the endomorphisms of the additive group scheme over L. We will denote such endomorphisms by additive polynomials in the variable X, and for ϕ to be a Drinfeld module it is further required that $\phi(a)$ has (1) linear part $i(a)X$ and (2) degree $q^{2\deg(a)}$ in X. Since all our Drinfeld modules will have rank two, we will omit references to the rank from now on. An endomorphism of ϕ is by definition an element $u \in \mathrm{End}(\mathbf{G}_a(\bar{F}))$ such that $u \circ \phi = \phi \circ u$. If F is finite, ϕ (or its j-invariant $j(\phi) = g^{q+1}/\Delta$) is said to be supersingular if its ring of endomorphisms is non-commutative.

Let L be a finite extension of K with ring of integers $\mathcal{O}$ (i.e., the integral closure of A in L), and ϕ a Drinfeld module over L. Assume that $\phi(T) = TX + gX^q + \Delta X^{q^2}$ for certain $g, \Delta \in \mathcal{O}$. For a prime $\mathfrak{B}$ of $\mathcal{O}$ not dividing Δ it makes sense to consider the reduction of ϕ mod $\mathfrak{B}$ as a Drinfeld module over the finite field $\mathcal{O}/\mathfrak{B}$, and $\mathfrak{B}$ is said to be a prime of supersingular reduction of ϕ if its reduction is supersingular.

Definition. We say that a non-zero algebraic integer j over K is (k, L)-*lifting* for an integer k and a finite extension L of K if $j = j(z)$ for some zero z of $E_{q^k - 1}$.

Theorem S. *Let L/K be a Galois extension of degree $[L : K]$ with ring of integers $\mathcal{O}$. Assume that $\phi(T) = TX + gX^q + \Delta X^{q^2}$ is a Drinfeld module with $g, \Delta \in \mathcal{O}$. If $j = j(\phi) \in \mathcal{O}$ is integral non-zero, then for any $k \geq 1$, either j is (k, L)-lifting, or*

$$\sum_{\deg(\mathfrak{p}) \leq k} f(\mathfrak{p}) \deg(\mathfrak{p}) s(\mathfrak{p}) \leq m(k) \cdot \max\{q[L : K], \log_q |\mathcal{O}/j|\},$$

where $\mathfrak{p}$ runs over the primes of A, $f(\mathfrak{p})$ is the residue degree of $\mathfrak{p}$, and $s(\mathfrak{p})$ is the number of supersingular primes of $\mathcal{O}$ not dividing g, Δ, which lie above $\mathfrak{p}$.

The theorem should be contrasted with the asymptotic results of Brown ([3]). The inequality in theorem S imposes restrictions on the number of supersingular invariants of a *fixed* degree. The point is that theorems E1-E3 show that j is only very rarely (k, L)-lifting. Theorem E1 implies that such liftings have degree q. Theorem E2 (or rather, (4.2)) implies in particular that the only (k, K)-lifting j-invariant is $j = T^q - T$ for $k = 2$ (this is the case considered in [6]). More generally, if $[L : K] < m(k)$, then there are no (k, L)-lifting elements in L.

One can also combine theorem S and theorem E2 for families of j-invariants. If $\{j_1, ..., j_n\}$ is a set of distinct j-invariants in L which do not satisfy the bound in theorem S for a certain even k, then forcedly

$$n \leq m(k) \text{ and } [K(j_1, ..., j_n) : K] \geq n!/2.$$

For example, making a few crude estimates shows that for at most q^2+1 integral j-invariants, the number of supersingular primes $\mathfrak{B}$ in $\mathcal{O}$ that lie above a prime of degree 4 in A is larger then $> (q^5)/4$.

One can interpret theorem S as follows: let ρ be the representation of the absolute Galois group of L on the $(\mathfrak{B} \cap A)$-torsion of the Drinfeld module. Theorem S imposes restrictions upon the number of primes $\mathfrak{B}$ for which the restriction of ρ to the decomposition group at $\mathfrak{B}$ is not ordinary.

Let us finally remark that a Drinfeld module can (by definition) have good reduction at a prime $\mathfrak{B}$ not dividing the global discriminant Δ, namely if it does not divide the $\mathfrak{B}$-local minimal discriminant. Hence there can be more supersingular primes then the ones considered above. If ϕ admits a global minimal model (*e.g.* if the class number of L is one), we can apply the theorem to it, and the problem does not occur. We will not pursue this topic any further (but compare [6], (1.4)).

2. The polynomials P_k

This section presents a short reminder on the polynomials P_k as they were introduced in [5]. It is our policy to give brief indications of the proofs, and refer to that reference for details. It follows from the theory of Drinfeld modules that g has a simple zero at the elliptic point $j = 0$ and nowhere else, and that Δ has a simple zero at the cusp of $GL(2, A)$ and is non-zero on Ω. The modular *function*

$$f_k(z) = (-1)^{k-1} \prod_{i \leq k} \langle i \rangle g(z)^{-\chi(k)} \Delta(z)^{-m(k)} E_{q^k-1}(z)$$

has no poles on Ω, and hence is a polynomial in $j(z)$. This turns out to be our polynomial P_k: $f_k(z) = P_k(j(z))$. There exists a recursion formula connecting the Eisenstein series E_{q^k-1}, and by retranslating it we find:

(2.1) Recursion Formula. *$P_k(j) \in A[j]$ is a polynomial satisfying the recursion $P_0 = P_1 = 1$ and for $k \geq 2$:*

$$P_k(j) = j^{d(k)} P_{k-1} - \langle k-1 \rangle P_{k-2}, \text{ with } d(k) = \frac{q^{k-1} + (-1)^k}{q+1}. \square$$

(2.2) Examples.

$$\begin{aligned} P_2(j) &= j - \langle 1 \rangle, \quad P_3(j) = j^q - \langle 1 \rangle j^{q-1} - \langle 2 \rangle, \\ P_4(j) &= j^{q^2+1} - \langle 1 \rangle j^{q^2} - \langle 2 \rangle j^{q^2-q+1} - \langle 3 \rangle j + \langle 1 \rangle \langle 3 \rangle, \\ P_5(j) &= j^{q^3+q} - \langle 1 \rangle j^{q^3+q-1} - \langle 2 \rangle j^{q^3} - \langle 3 \rangle j^{q^3-q^2+q} \\ &\quad + \langle 1 \rangle \langle 3 \rangle j^{q^3-q^2+q-1} - \langle 4 \rangle j^q + \langle 1 \rangle \langle 4 \rangle j^{q-1} + \langle 2 \rangle \langle 4 \rangle. \end{aligned}$$

(2.3) Theorem E1. *The roots of P_k have absolute value q^q. The zeros of E_{q^k-1} in the domain $\{z \in \Omega : |z| = \inf\{|z-a| : a \in A\} \geq 1\}$ (to which any point of Ω can be mapped by $GL(2,A)$) are on the "unit circle" $|z| = 1$. They are simple and transcendental over K.*

Sketch of proof. The first statement follows from the fact that the Newton polygon of P_k for the valuation $-\deg$ is a straight line of slope q: if we write

$$P_k(j) = \sum_{i=0}^{m(k)} c_i^{(k)} j^{m(k)-i},$$

then

(2.3.1) $\quad |c_i^{(k)}| = q^{qi}$ if $c_i^{(k)} \neq 0$.

(This is verified inductively using the recursion formula.) The second statement follows from estimates relating $|j(z)|$ and $|z|$. A theorem of Yu [22] implies that non-transcendental zeros of E_{q^k-1} have complex multiplication. An estimate for the j-invariants of such CM-points by Brown ([3], (2.8.2)) shows that they never have absolute value q^q. Finally, the proof that the zeros are simple is a generalization of the one give for $k = 1$ by Gekeler ([10], VII.3.3). It will also follow independently from (4.2). $\square$

(2.4) Proposition. *The Galois group of P_3 is the affine group $AGL(1, \mathbf{F}_q)$.*

Proof. After inversion $Y = j^{-1}$ of the variable, the polynomial is of the form $Y^q + aY + b$, and it is easy to see that the splitting field is a tower of the cyclic extension $K(\sqrt[q-1]{-a})$ of K with an Artin-Schreier extension. $\square$

(2.5) Proposition. *Let $\mathfrak{p}$ be a prime of degree n in A. Then the following congruences hold:*

$$\forall k \geq 0: \quad P_{k+n} = j^{\chi(k)d(n+1)} P_k^{q^n} P_n \ \mathit{mod}\ \mathfrak{p}.$$

Proof. Using recursion and the fact that $\langle k+n-1 \rangle \equiv \langle k-1 \rangle^{q^n} \bmod \mathfrak{p}$. $\square$

(2.6) Proposition (Gekeler [11] section 5). *Let $\mathfrak{p}$ be a prime of degree k in A. Then $j^{\chi(k)}P_k(j)$ mod $\mathfrak{p}$ is the supersingular polynomial for rank 2-Drinfeld modules modulo $\mathfrak{p}$, i.e., its roots are the supersingular j-invariants over $A/\mathfrak{p}$.*$\square$

(2.7) Proposition (Gekeler [9] (5.6), [10] (3.7), (6.4)). *The supersingular polynomial modulo $\mathfrak{p}$ has simple roots, factorizes over $A/\mathfrak{p}$ into the product of linear and quadratic factors, and for k even, the number $Q_\mathfrak{p}$ of quadratic factors of the supersingular polynomial satisfies*

$$4Q_\mathfrak{p} = 2m(k) - h(e\mathfrak{p}),$$

where e is some non-square in $\mathbf{F}_q$, and $h(\cdot)$ indicates the class number of $A[\sqrt{\cdot}]$.$\square$

3. Resources from group theory and Galois theory

(3.1) Proposition. *Let F be a local field of residual characteristic p, f an Eisenstein polynomial over F of degree n, coprime to p. Then the inertia group of the splitting field of f is generated by an n-cycle.*

Proof. Let α be a root of f. The extension $F(\alpha)/F$ is totally ramified of degree n, and since $(n,p) = 1$ we have $F(\alpha) = F(\sqrt[n]{\pi})$ for some uniformizing element $\pi \in F$. The normal closure of $F(\alpha)$ is $L := F(\alpha)(\zeta_n)$, where ζ_n is a primitive n-th root of unity.

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash] \arrow[dr, dash, "\mathbf{Z}/n"] & \\ F(\alpha) & & F(\zeta_n) \\ & F \arrow[ul, dash, "n"] \arrow[ur, dash] & \end{tikzcd}$$

Since $(n,p) = 1$, the extension $F(\zeta_n)/F$ is unramified, and hence $F(\zeta_n)$ and $F(\alpha)$ are linearly disjoint. Hence $[L : F(\zeta_n)] = [F(\alpha) : F] = n$, so f is irreducible over $F(\zeta_n)$. But $\mathrm{Gal}(L/F(\zeta_n))$ is the inertia group of L/F, and hence cyclic of order n since $(n,p) = 1$ (e.g. [18], IV.2 Cor. I). Since f is irreducible over $F(\zeta_n)$, this cyclic group is also transitive on the n roots of f. Hence it is generated by an n-cycle. $\square$

(3.2) Proposition. *A transitive permutation group of degree n, containing a subgroup that acts transitively on $d > \frac{n}{2}$ letters, and stabilizes the other letters, such that d and n are coprime, is primitive.*

Proof. Assume that G acts transitively on $\Omega = \{1, ..., n\}$ as a permutation group, and H is a subgroup of G acting transitively on $D = \{1, ..., d\}$, where $d > \frac{n}{2}$, but fixes $\Omega - D$. Let B be a non-trivial block for G. We can assume that $|B| \leq \frac{n}{2}$.

Assume that $\{i, j\} \in B$ for some $i \leq d$ and $j > d$ (such $j > d$ exists since $d < n$). Then for all $h \in H : hj = j \in B \cap hB$, so $H \cdot B = B$ (since B is a block). But $D = H \cdot \{i\} \subseteq H \cdot B = B$, so $d < |B| \leq \frac{n}{2}$, a contradiction.

Hence either $B \subseteq D$ or $B \subseteq \Omega - D$. Since G is transitive, translates of B are blocks that cover Ω. Finally, $|B|$ has to divide both $|D| = d$ and $|\Omega| = n$. □

(3.3) Proposition (Jordan). *A primitive permutation group of degree n containing an m-cycle ($m > 1$) is at least $n - m + 1$-transitive.*

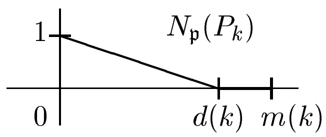
Remark. This theorem is frequently attributed to Marggraff, although it appears to have been stated first by Jordan. For some history and an up-to-date proof, one can consult [15], *pp.* 273-274. □

(3.4) Proposition (Wielandt [21] (a)). *The degree of transitivity t of a permutation group of degree n not containing A_n is bounded by $t < 3 \log n$.*

Remark. Alternatively, it follows from the classification of finite simple groups that $t < 6$. □

4. Proof of theorem E2

(4.1) $\mathrm{Gal}(P_k)$ *contains a $d(k)$-cycle.* Let $\mathfrak{p}$ be a prime of degree $k-1$ in A. The Newton polygon of P_k over the completion $K_\mathfrak{p}$ consists of a segment from $(0,1)$ to $(d(k),0)$ and a segment from $(d(k),0)$ to $(m(k),0)$.



As the first segment contains no lattice points, P_k must factor as $P_k = fg$ over $K_\mathfrak{p}$, where f is an Eisenstein polynomial of degree $d(k)$. Since $P_k = j^{d(k)} P_{k-1} \bmod \mathfrak{p}$, it follows that $g \bmod \mathfrak{p}$ is the supersingular polynomial for $\mathfrak{p}$, and hence has no multiple roots by (2.7). So elements of the inertia group $I(P_k/\mathfrak{p})$ of P_k over $K_\mathfrak{p}$ act trivially on the roots of g. Hence $I(P_k/\mathfrak{p}) \cong I(f/\mathfrak{p})$.

Since $d(k)$ and q are coprime, lemma (3.1) on local fields implies that the inertia group of f at $\mathfrak{p}$ is cyclic, generated by a $d(k)$-cycle. By the above, we find it in the inertia group of P_k at $\mathfrak{p}$, and *a fortiori* in the Galois group of P_k.

(4.2) *Irreducibility.* Suppose that $P_k = fg$ for two factors $f, g \in A[j]$. In the previous paragraph, we have already found an irreducible factor of P_k of degree $d(k)$ over the completion of K at a prime of degree $k-1$, and hence one can assume that $\deg f \geq d(k)$. For any prime $\mathfrak{p}$ of degree $k-1$ in A, there is a factorization $P_k = f_\mathfrak{p} g_\mathfrak{p}$ over $K_\mathfrak{p}$, with $f_\mathfrak{p}$ irreducible of degree $d(k)$. For reasons of degree, g divides $g_\mathfrak{p}$, and since $g_\mathfrak{p} = P_{k-1} \bmod \mathfrak{p}$, one finds that g divides $P_{k-1} \bmod \mathfrak{p}$. Let α be a root of g; it follows that

$$P_{k-1}(\alpha) = \mathfrak{a} \prod \mathfrak{p}$$

holds in $A[\alpha]$, for some integral element $\mathfrak{a}$, where the product runs over all irreducible $\mathfrak{p}$ of degree $k-1$ in A.

Assume that $\mathfrak{a} \neq 0$. Since $P_k(\alpha) = 0$, it follows from (2.3) that $|\alpha| = q^q$, and by (2.3.1), the coefficient of $j^{m(k-1)-i}$ in P_{k-1}, if it is non-zero, has absolute value q^{qi}. Hence we see that all terms of $P_k(\alpha)$ have absolute value $q^{m(k-1)}$. Finally,

$$\log_q |\mathfrak{a}| + \log_q |\prod \mathfrak{p}| = \log_q |P_{k-1}(\alpha)| \leq qm(k-1).$$

On the other hand,

$$\log_q |\mathfrak{a}| \geq 0, \quad \log_q |\prod \mathfrak{p}| = (k-1)N(k-1),$$

where $N(k-1)$ is the number of primes of degree $k-1$ in A. We claim that

$$qm(k-1) < (k-1)N(k-1).$$

This statement is equivalent to

$$q^{k-2} + q^{k-4} + ... + q^{2-\chi(k)} < \sum_{d|k-1} \mu(\frac{k-1}{d}) q^d = q^{k-1} + ...,$$

(where μ is the Möbius function). This, however, is clear from considering the numbers in the inequality as q-adic expansions (On the right hand side, the only q-adic digits occurring are ± 1, and $q > 2$).

In conclusion, $\mathfrak{a} = 0$, so α is a root of both P_{k-1} and P_k. Hence by using the recursion (2.1) in the opposite direction, one finds inductively that $P_1(\alpha) = 0$, a contradiction. So g has no root, *i.e.* it is constant. □

(4.3) *Group theory, revisited.* By (4.2), the Galois group of P_k is transitive as a permutation group on the roots, and the $d(k)$-cycle of (4.1) generates a cyclic subgroup which acts transitively on $d(k) > \frac{m(k)}{2}$ roots and leaves the rest fixed. For k even, $d(k)$ and $m(k)$ are coprime since $qd(k) + (1-q)m(k) = 1$. By (3.2), we conclude that $\mathrm{Gal}(P_k)$ is primitive. Since it also contains a $d(k)$-cycle, one obtains from (3.3) that it is $(m(k) - d(k) + 1) = (m(k-1) + 1)$-transitive. Since $m(k-1) + 1 \geq 3 \log m(k)$ for $k > 3$, it follows from (3.4) that $\mathrm{Gal}(P_k)$ contains the alternating group of degree $m(k)$.

So far, we have shown the first part of theorem E2: *if k is even, $Gal(P_k)$ is alternating or symmetric.*

(4.4) *An odd element in the Galois group.* To decide in favour of $S_{m(k)}$ instead of $A_{m(k)}$, we will produce an odd element in the Galois group by using theorem H.

Assume first of all that k is divisible by 8. By (2.7), primes $\mathfrak{p}$ of degree k in A are unramified in any root field of P_k, and their decomposition group is generated by a product of $Q_\mathfrak{p}$ transpositions. Hence there is an odd element in $\mathrm{Gal}(P_k)$ if we can show that $Q_\mathfrak{p}$ is odd for some $\mathfrak{p}$. Since $m(k)$ is constant if k is, it suffices (again by (2.7)) to show that there exist a non-square $e \in \mathbf{F}_q$ and primes $\mathfrak{p}, \mathfrak{p}'$ of degree k in A with $h(e\mathfrak{p}) \not\equiv h(e\mathfrak{p}')$ mod 8. But under the conditions in the statement of theorem E2, this follows from theorem H, which will be proved in the next section.

Finally, assume that $k = 2 \bmod 8$. Then for any prime $\mathfrak{q}$ of degree $k-2$ in A we have that

$$P_k(j) = (j - \langle 1 \rangle)^{q^{k-2}} P_{k-2}(j) \bmod \mathfrak{q},$$

and the corresponding Newton polygon consists of a segment from $(0,1)$ to $(q^{k-2},0)$ and a segment from $(q^{k-2},0)$ to $(m(k),0)$. In this case, $k-2$ is divisible by 8. By the previous argument, we can find a $\mathfrak{q}$ such that $Q_\mathfrak{q}$ is odd. The corresponding product $\bar{\tau}$ of $Q_\mathfrak{q}$ transpositions in $\mathrm{Gal}(P_{k-2} \bmod \mathfrak{q})$ lifts to an element $\sigma\tau$ of $\mathrm{Gal}(P_k/K_\mathfrak{q})$ where σ is in the inertia group of $\mathfrak{q}$ by the above congruence (a similar argument was used at the end of (4.1)). Hence also the (odd) element τ belongs to $\mathrm{Gal}(P_k)$. This finishes the proof. □

5. Proof of theorem H

(5.1) *Genus theory* (E. Artin [2], section 11). Let $L = K(\sqrt{e\mathfrak{p}})$ and let $\mathcal{C}$ denote the 2-primary part of the class group of L. Then $\mathcal{C}$ is a cyclic 2-group (since the discriminant has only one monic prime divisor). It is trivial if and only if $\deg(\mathfrak{p})$ is odd (*loc. cit.*, Satz). If $\deg(\mathfrak{p})$ is even, then the two-torsion of $\mathcal{C}$ is generated by the "ambiguous class" $\mathcal{A}$, constructed as follows: consider the quadratic form

$$\kappa(X,Y) = eX^2 + \alpha XY + Y^2,$$

where $\alpha \in \mathbf{F}_q$ is chosen such that κ is irreducible. If $(B,C) \in A$ are such that

$$e\mathfrak{p} = \kappa(B,C) \text{ with } \deg B < \deg C = \frac{k}{2},$$

then in fact $\mathcal{A}$ is the class of the ideal $(C, B + \sqrt{e\mathfrak{p}})$ of K-norm C. We will let $\mathcal{C}^i$ denote the groups $\{c^i | c \in \mathcal{C}\}$.

(5.2) Proposition. *Fix a non-square $e \in \mathbf{F}_q$. For a prime $\mathfrak{p}$ of degree k in A, the class number of $K(\sqrt{e\mathfrak{p}})$ is even if and only if k is, and is divisible by 4 if and only if k is.*

Proof. The parity of the class number follows immediately from the genus theory in (5.1). The statement about divisibility by 4 follows from (2.7): 4 divides $h(e\mathfrak{p})$ if and only if $m(k)$ is even (recall that k is even then). By an elementary argument, $m(k) = \frac{k}{2} \bmod 2$.

One can give a different proof using class field theory. We take our inspiration from [20].

$$\begin{tikzcd}
 & H^{\mathcal{C}^4} \arrow[d, dash, "?\ (2\text{ or }4)"'] \arrow[ddr, dash, "R_\mathfrak{p}/R_\mathfrak{p}^2\ (\ ?\ |\cdot| = 2\text{ or }4)"] & \\
 & H^{\mathcal{C}^2} \arrow[dl, dash, "2"'] \arrow[dr, dash] & \\
K(\sqrt{e\mathfrak{p}}) \arrow[dr, dash, "2"'] & & K(\sqrt{e}) \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

If H is the Hilbert class field of L (this means that ∞ is totally split), then 4 divides the class number if and only if $[H^{\mathcal{C}^4} : H^{\mathcal{C}^2}] = 2$. Since the genus field $H^{\mathcal{C}^2}$ equals $L(\sqrt{e})$, this is equivalent to $[H^{\mathcal{C}^4} : K(\sqrt{e})] = 4$. But the Galois group of this extension is $R_{\mathfrak{p}}/R_{\mathfrak{p}}^2$, where $R_{\mathfrak{p}}$ is the ray class group of K at $\mathfrak{p}$.

If $\mathfrak{p}$ splits as $\pi.\pi'$ in $K(\sqrt{e})$, then this ray class group is by class field theory equal to

$$R_{\mathfrak{p}} = (A[\sqrt{e}]/\pi)^* \times (A[\sqrt{e}]/\pi')^*/\mathbf{F}_q^*(\sqrt{e}).$$

So 4 divides the class number if and only if $\sqrt{e}$ is a square modulo π, if and only if $2|\deg(\pi)$, if and only if $4|k$. □

(5.3) *Proof of theorem H.* The cyclic structure of $\mathcal{C}$ implies that $h(e\mathfrak{p})$ is divisible by 8 if and only if $\mathcal{A} \in \mathcal{C}^4$. We will now proceed to construct, for k divisible by 8 and q large enough, two pairs (B,C) and (B',C') which in the sense of section (5.1) correspond to primes $\mathfrak{p}$ and $\mathfrak{p}'$ with class numbers of different 8-rank.

During the construction, use will be made of the following fact:

(5.3.1) Proposition. *Suppose that f and g are mutually coprime monic polynomials over a finite field of q^2 elements with $l = \deg f > \deg g$, such that $fg^{-1} \notin \mathbf{F}_{q^2}(T^p)$. Assume that the Galois group of $f - tg$ over $\mathbf{F}_{q^2}(t)$ contains an l-cycle, and the splitting field contains no constant extension of $\mathbf{F}_{q^2}$. Then there is a constant C_l only depending on l such that for $q > C_l$, there exists at least one $\delta \in \mathbf{F}_{q^2}$ such that $f - \delta g$ is irreducible over $\mathbf{F}_{q^2}$.*

Proof. This is a special case of theorem 1 in [4]. □

Notation. Throughout the rest of this paragraph, we will denote $\frac{k}{2}$ by l.

(5.3.2) *Construction of (B,C).* We set $C = T^l$. Since T splits in L/K, we see that $\mathcal{A}$ is the l-th power of an ideal in L above T. Since l is divisible by 4, we have $8|h(e\mathfrak{p})$ *if* we can construct a B such that the corresponding $\mathfrak{p}$ is irreducible over K. The form κ factors as

$$\kappa(X,Y) = e(X - \delta_+ Y)(X - \delta_- Y) \text{ over } \mathbf{F}_{q^2},$$

where $2e\delta_\pm = \alpha \pm \sqrt{\alpha^2 - 4e}$. Hence we find an irreducible $\mathfrak{p}$ in A with the desired properties if we can show the following:

(*) There exists $\delta \in \mathbf{F}_{q^2}$ and $B \in \mathbf{F}_q[T]$ $(\deg B < l)$ such that $T^l - \delta B(T)$ is irreducible over $\mathbf{F}_{q^2}$,

by choosing an appropriate α once δ has been chosen.

Fix a non-trivial B such that $B(0) \neq 0$ and BT^{-l} is not a rational function of T^p. Consider the polynomial $f := T^l - tB(T)$ over $\mathbf{F}_{q^2}(t)$. It is an Eisenstein polynomial for the prime t of $\mathbf{F}_{q^2}[t]$, and hence its Galois group contains an l-cycle if q and l are coprime (by (3.1)). By proposition (5.3.1), claim $(*)$ follows.

(5.3.3) *Construction of (B',C').* We choose $C' = T^{l-2}Q(T)$, where Q is quadratic irreducible in A. Suppose that $\mathcal{E}$ and $\mathcal{L}$ are two prime factors in the respective splitting of T and Q in L/K. Then the ambiguous class is

$\mathcal{A} = \mathcal{E}^{l-2}\mathcal{L}$, and hence the class number $h(e\mathfrak{p}')$, where $\mathfrak{p}'$ is associated to a pair (B', C'), is divisible by 8 if and only if $\mathcal{E}^2\mathcal{L} \in \mathcal{C}^4$. Since $\mathcal{E}$ and $\mathcal{L}$ are non-split in the genus field $L(\sqrt{e})$ of L (with Galois group $\mathcal{C}/\mathcal{C}^2$), $\mathcal{E}$ and $\mathcal{L}$ do not belong to $\mathcal{C}^2$. Suppose that σ is a generator of $\mathcal{C}$. Then $\mathcal{E} = \sigma^{2r+1}$ and $\mathcal{L} = \sigma^{2s+1}$ for some $r, s \in \mathbf{Z}$. Hence $\mathcal{E}^2\mathcal{L} \notin \mathcal{C}^4$, and $h(e\mathfrak{p}')$ is not divisible by 8. Left to show is the following statement:

(**) There exists $\delta \in \mathbf{F}_{q^2}$ and $B \in \mathbf{F}_q[T]$ $(\deg B < l)$ such that $T^{l-2}Q(T) - \delta B(T)$ is irreducible over $\mathbf{F}_{q^2}$.

This will follow once again from proposition (5.3.1) if we can show that there exists a B such that $\mathrm{Gal}(f/\mathbf{F}_{q^2}(t))$ contains an l-cycle, where $f = T^{l-2}Q(T) - tB(T)$. If $B(T)$ is not divisible by T nor $Q(T)$, then since the polynomial is linear in t, Gauß' lemma implies that it is irreducible over $\mathbf{F}_{q^2}(t)$. On the other hand, if $l-2$ and q are coprime, then (3.1) implies that the Galois group contains an $(l-2)$-cycle σ. The argument is similar to the one used in (4.1): $f = T^{l-2}Q(T) \bmod t$, Q has no multiple roots, and the Newton polygon of f over the t-completion has the corresponding form (a segment from $(0,1)$ to $(l-2,0)$ and a segment from $(l-2,0)$ to $(l,0)$).

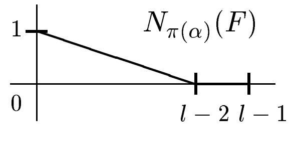
We will now prove that for $B = 1$, the Galois group of f is primitive. Let $f := T^{l-2}Q(T) - t$ for some quadratic irreducible $Q(T) = T^2 + aT + b$. Remark that it suffices to show that $\mathrm{Gal}(f)$ is 2-transitive ([21] (b), Theorem 9.6). It suffices to show that the stabilizer of any root α of f is transitive. We now appeal to the following "twisted derivative"-trick of Abhyankar's ([1], par. 18), which says that this stabilizer is

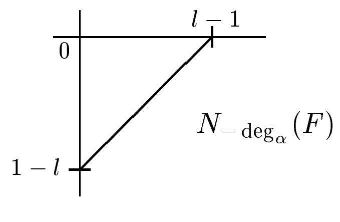
$$\mathrm{Gal}(F/\mathbf{F}_{q^2}(\alpha)), \text{ where } F = \frac{T^lQ(T) - \alpha^lQ(\alpha)}{T - \alpha}.$$

It is easy to compute that

$$F = T^{l-1} + (\alpha + a)T^{l-2} + \sum_{i=0}^{l-3} Q(\alpha)\alpha^iT^{l-3-i}.$$

All we have to show is that F is irreducible over $\mathbf{F}_{q^2}(\alpha)$. Recall that α is transcendental over $\mathbf{F}_q$. If π is an irreducible factor of Q over $\mathbf{F}_{q^2}$, then the Newton polygon of F for $\pi(\alpha)$ contains a straight line from $(0,1)$ to $l-2$. Hence either F is irreducible, or it has a root, which is not divisible by $\pi(\alpha)$. The Newton polygon of F for the valuation $-\deg_\alpha$ is a straight line from $(0, -l+1)$ to $(l-1, 0)$, so a possible root T_0 of F is linear in α.





Because the only possible prime divisors of T_0 occur in the constant $F(0) = \alpha^{l-3}Q(\alpha)$, it has to be of the form $T_0 = \beta\alpha$ for some $\beta \in \bar{\mathbf{F}}_q^*$. If we set

$$s = \sum_{i=0}^{l-1} \beta^i, \text{ then } \alpha^{3-l}F(T_0) = s\alpha^2 + a(s - \beta^{l-1})\alpha + b(s - \beta^{l-1} - \beta^{l-2}) = 0.$$

It follows that $\beta = 0$, a contradiction. Hence there is no root, and this proves our claim.

So $\mathrm{Gal}(f)$ is primitive, and contains an $(l-2)$-cycle. If it is not $(l-1)$-transitive, then it has a proper Jordan set of size $l-2$. (Recall that a Jordan set J of a permutation group G on a set Ω is a non-trivial subset of Ω such that the pointwise stabilizer of the complement acts transitively on it, and a Jordan set is called proper if the cardinality of its complement is strictly less then the transitivity degree of G). Assuming the classification of finite groups, one can go through the list of such groups G (published in [15], p. 276) acting on Ω with proper Jordan set J:

G	Ω	$\Omega - J$
$\leq A\Gamma L(d,q)$	$AG(d,q)$	affine subspaces
$\leq P\Gamma L(d,q)$	$PG(d,q)$	projective subspaces
A_7	$PG(3,2)$ of degree 15	of size 3
$2^4 \cdot \hat{A}_7$	$AG(4,2)$ of degree 16	of size 4
$M_{22}, M_{23}, M_4, \mathrm{Aut}(M_{22})$	Steiner systems of degrees 22,23,24,22	of size 6,7,8,6

The difference between the degree $|\Omega|$ of G and the size of J is always larger then 2. Hence the degree of transitivity of $\mathrm{Gal}(f)$ is larger then $l-2$. Since the $(l-2)$-cycle is of even length, $\mathrm{Gal}(f)$ is symmetric, and thus it contains an l-cycle. □

(5.4) *Remark.* The (classical) study of 8-divisibility of the class number of $\mathbf{Q}(\sqrt{-p})$, which goes back to a letter of Gauß to Dirichlet (dated May 30, 1828, *see* [7]), depends on the fact that the 2-torsion in the class group is generated by the prime ideal above 2. In particular, the norm of the ambiguous class is independent of p, whereas for function fields, that norm C depends on $\mathfrak{p}$. Thus the extra non-trivial problem of the construction of irreducibles in A of a prescribed form (which we have encountered in the form: given C, construct a prime $\mathfrak{p}$ such that $K(\sqrt{e\mathfrak{p}})$ has this C as norm of the ambiguous class) arises.

6. Supersingularity

(6.1) Proposition (Gekeler, [9]). *Let ϕ be a Drinfeld module over a finite field F equipped with an A-algebra structure $i : A \to F$. Let $\mathfrak{i} = \ker(i)$. Then ϕ is supersingular if and only if the coefficient of $X^{q^{\deg(\mathfrak{i})}}$ in $\phi(\mathfrak{i})$ is zero.* □

(6.2) Proposition. *Let ϕ be a Drinfeld module over a finite extension L of K, and assume that $\phi(T) = TX + gX^q + \Delta X^{q^2}$ for some $g, \Delta \in \mathcal{O}$, where $\mathcal{O}$ is the ring of integers of L. Set $j = g^{q+1}/\Delta$. Let $\mathfrak{B}$ be a prime ideal of $\mathcal{O}$,* *not dividing Δ, and set $\mathfrak{p} = \mathfrak{B} \cap A$. Let $l_{\mathfrak{p}}(g, \Delta)$ be the coefficient of $X^{q^{\deg(\mathfrak{p})}}$ in $\phi(\mathfrak{p})$. Then:*

(i) $\mathfrak{B}$ is a supersingular prime of ϕ if and only if $l_{\mathfrak{p}}(g, \Delta) = 0$ mod $\mathfrak{B}$.

(ii) ("Deligne's congruence") $l_{\mathfrak{p}}(g, \Delta) = P_{\deg \mathfrak{p}}(j)\Delta^{m(k)} g^{\chi(k)}$ mod $\mathfrak{B}$.

Proof. The first part follows immediately from (6.1). For $L = K$, part (ii) is the contents of theorem (11.5) in [11]. The proof is inductive, using the recursion formula for P_k. A careful inspection of the arguments show that they go through in our setting. □

(6.3) *Proof of theorem S.* Let $\phi, g, \Delta, j, L, \mathcal{O}$ be as in the statement of the theorem. Assume S is the set of supersingular primes $\mathfrak{B}$ for ϕ, such that $\mathfrak{B} \cap A$ is of degree $i \leq k$, not dividing g, Δ. Since $\mathfrak{B}$ does not divide g and Δ, we find by (6.2) that

$$P_i(j) = 0 \text{ mod } \mathfrak{B}.$$

Now the congruences in (2.5) also hold modulo $\mathfrak{B}$ (an easy check), so the previous formula implies that $\mathfrak{B} | P_k(j)$. Taking everything together, we find that the following inclusion of ideals holds:

$$P_k(j) \cdot \mathcal{O} \subseteq \prod_{\mathfrak{B} \in S} \mathfrak{B}$$

since the different $\mathfrak{B}$ are coprime. If we define $\deg_{\mathcal{O}}$ by $\deg_{\mathcal{O}}(\mathfrak{A}) = \log_q |\mathcal{O}/\mathfrak{A}|$ (i.e., the extension of the degree-function on $\mathcal{O}$ to the non-zero ideals of $\mathcal{O}$), then the above implies that either $P_k(j) = 0$, so j is (k, L)-lifting, or

$$\deg_{\mathcal{O}}(P_k(j)) \geq \sum_S \deg_{\mathcal{O}}(\mathfrak{B}).$$

Using (2.3.1), we find that

$$\deg_{\mathcal{O}}(c_i^{(k)}) = [L : K] \deg(c_i^{(k)}) = [L : K]qi,$$

and a small computation gives that

$$\deg_{\mathcal{O}}(P_k(j)) \leq m(k) \cdot \max\{q[L : K], \log_q |\mathcal{O}/j|\}.$$

On the other hand,

$$\deg_{\mathcal{O}}(\mathfrak{B}) = f(\mathfrak{B}) \deg(\mathfrak{B} \cap A),$$

where $f(\mathfrak{B}) = [\mathcal{O}/\mathfrak{B} : A/(\mathfrak{B} \cap A)]$ is the residue degree of $\mathfrak{B}$. If we assume that L/K is Galois, and put everything together, we find

$$\sum_{\deg(\mathfrak{p}) \leq k} f(\mathfrak{p}) \deg(\mathfrak{p}) s(\mathfrak{p}) \leq m(k) \cdot \max\{q[L : K], \log_q |\mathcal{O}/j|\},$$

where $f(\mathfrak{p})$ is the residue degree of $\mathfrak{p}$, and $s(\mathfrak{p})$ is the number of supersingular primes $\mathfrak{B}$ not dividing g, Δ and lying above $\mathfrak{p}$ in $\mathcal{O}$. □

Stockage diophantien et hypothèse ABC généralisée

Résumé Soit (L, M, ϕ) un triple consistant d'un langage du premier ordre L, et un ensemble M qui admet une interprétation ϕ de L. On définit la relation de sous-structure positive-existentielle pour deux tels triples, qui généralise la notion d'ensemble positif-existentiel. Si un triple admet son propre produit cartésien $(L, M \times M, \phi \times \phi)$ comme sous-structure, nous disons qu'il admet stockage positif-existentiel. Ceci généralise la notion de fonction de stockage, connu de la théorie de récursion. On démontre que $\mathbf{Z}$ et certains corps de fonctions admettent stockage positif-existentiel.

Diophantine storing and the generalized ABC-hypothesis

Abstract Let (L, M, ϕ) be a triple consisting of a first order langage L and a set M that allows an interpretation ϕ of L. We define the relation of positive existential substructure for two such triples, which generalizes the notion of positive existential set. If a triple allows its proper cartesian product $(L, M \times M, \phi \times \phi)$ as substructure, we say it admits positive-existential storing. This generalizes the notion of a storing function, known from recursion theory. We then prove that $\mathbf{Z}$ and certain rational function fields admit positive existential storing.

1. DÉFINITIONS. – Soit (M, L, ϕ) un triple consistant d'un langage du premier ordre L, spéfiée par des prédicats (constantes, opérations, relations) $\{P_{i,\alpha}\}$ i-aire, un ensemble M et une interprétation ϕ de L dans M ([27]). Toutes les caractères romaines, indexées par des nombres naturels, sont admises comme variables si elles ne figurent pas dans les prédicats. Souvent, nous omettrons ϕ de la notation. Nous considérons l'interprétation $\phi(P_{i,\alpha})$ d'un prédicat comme sous-ensemble de M^i. Une formule de L est appelée *positive-existentielle* (p.e.) si elle est de la forme $(\exists x)a$ oú x est une liste de variables et a est une formule sans négations et quantificateurs. Une telle formule est dite *diophantienne* (d.) si a est atomique. Un sous-ensemble $S \subseteq M^r$ $(r \in \mathbf{Z}_{>0})$ est dit *p.e. (resp. d.) ϕ-définisable* s'il y a une formule p.e. (resp. d.) f dans L qui décide l'appartenance à S (en termes de ϕ-vérité). Nous disons d'un autre tel triple $(M', L' = \{P'_{i,\alpha}\}, \phi')$ qu'*il est p.e. (resp. d.) dans* (M, L, ϕ) s'l y a une injection d'ensembles $M' \subseteq M$, tel que l'image est p.e. (resp. d.) ϕ-définisable, et les inclusions induites $\phi'(P'_{i,\alpha}) \subseteq M^i$ sont, eux aussi, p.e. (resp. d.) ϕ-définisable. Si, pour chaque pair de formules atomaires p, q dans L, l'interprétation de la formule $p \wedge q$ (resp. $p \vee q$) équivaut (en termes de ϕ-vérité) à une formule d., nous disons que le triple *admet* $\wedge$ (resp. $\vee$). Dans ce cas, la théorie p.e. du triple est équivalente à la théorie d. du triple.

2. *Examples. – Un sous-ensemble S p.e. ϕ-définisable est p.e. dans (M, L, ϕ) si on le considère comme triple $(S, L, \phi|_S)$, où $\phi|_S$ est la restriction de ϕ à S. Preuve:* Soit $(\exists y \in M) P_S(x, y)$ la formule p.e. qui équivaut a $x \in S$ (où $y = (y_1, ..., y_m)$ est une liste de variables). Soit P un prédicat de L. Alors $(x_1, ..., x_n) \in \phi|_S(P_i)$ équivaut a $(\exists y^{(j)}) \bigwedge_j P_S(x_j, y^{(j)}) \wedge P_i(x_1, ..., x_i)$, ce qui est p.e.

Soit R un anneau commutatif avec unité. De façon naturelle, il admet une interprétation pour chaque langage L donné par des prédicats $(c_0^{(i)}, +_3, \cdot_3, =_2)$, dont les indices indiquent l'arité, et $c_0^{(i)}$ sont des constantes arbitraires (moins en nombre que $|R|$). Examples typiques sont les nombres $(\mathbf{Z}, (0, 1, +, \cdot, =))$ et les polynômes $(\mathbf{R}[t], (0, 1, t, +, \cdot, =))$. Si R est sans diviseurs de zéro et il y a un polynôme f dont les coefficients sont interprétable pour L, et qui n'a pas de zéro dans R, alors R admet $\vee$ et $\wedge$. *Preuve*: Si p et q sont des polynômes, alors $R \models (p = 0 \vee q = 0) \iff (pq = 0)$, et $R \models (p = 0 \wedge q = 0) \iff q^{\deg(f)} f(p/q) = 0$.

3. Premières propriétés. – *Si $(M'', L'') \subseteq (M', L') \subseteq (M, L)$ est une chaîne d'inclusions p.e. (resp. d. et tel que (M, L) admet $\wedge$), alors l'inclusion $(M'', L'') \subseteq (M, L)$ est p.e. (resp. d.) Si, en outre, la théorie p.e. (resp. d.) de (M', L') est indécidable, le même vaut pour (M, L).* Les démonstrations sont faciles.

4. *Examples.* – Les résultats concernant le dixième problème d'Hilbert obtenus par Denef ([24], [25]) et Pheidas ([29]) s'interprêtent de la façon suivante dans notre terminologie: $(\mathbf{Z}, (0, 1, +, \cdot, =))$ est p.e. dans les polynômes $(R[t], (0, 1, t, +, \cdot, =))$, où R est anneau commutatif unitaire sans diviseurs de zéro, et dans les corps de fonctions $(k(t), (0, 1, +, \cdot, =))$ tel que k est formellement réel ou fini. Notons: nos définitions permettent de donner un sens précis à des questions comme type "Est $\mathbf{F}_q(t)$ diophantien dans $\mathbf{Q}$?".

5. Définition. – Soit (L, M, ϕ) un triple. Notons que le langage L admet aussi une interprétation naturelle ϕ^2 dans le produit cartésien M^2 de façon "diagonal" (c.-à-d., $\phi^2(P_{i,\alpha}) = \phi(P_{i,\alpha}) \times \phi(P_{i,\alpha}) \subseteq M^{2i}$). Nous disons que (M, L) admet *stockage p.e. (resp. d.)* si (M^2, L, ϕ^2) est p.e. (resp. d.) dans (M, L, ϕ). Notons que si $f : M^2 \to M$ est l'injection p.e. qui paraît, alors il ne faut point que $f(\phi^2(P_{i,\alpha})) = \phi(P_{i,\alpha})$.

6. Principe de construction. – *Soit R un anneau, et L un langage qui s'interprête dans R comme dans §2, et tel que (R, L) admet $\wedge$ et $\vee$. Supposons que les objects suivants existent: (a) un recouvrement disjoint fini $\{U_i\}_{i=0}^n$ de R^2, et (b) des injections polynômiales $f_i : U_i \to R$ dont les images sont disjointes et diophantiennes dans (R, L). Alors (R, L) admet stockage diophantien.*

Preuve. Soit $f : R^2 \to R$ l'injection définie par $f(x) = y \iff x \in U_i \wedge f_i(x) = y$, alors $\mathrm{im}(\phi)$ est diophantien dans (R, L), comme ceci admet $\vee$. Définisons une interpretation ϕ_f de L dans $\mathrm{im}(f)$. Soit P un prédicat de degré i dans L, alors

$$(y_1, ..., y_i) \in \phi_f(P) \subseteq R^i \iff \exists (x_{11}, x_{12}, ..., x_{i1}, x_{i2}) \in R^{2i} :$$
$$\bigwedge_{j=1}^{i} y_j = f(x_{j1}, x_{j2}) \wedge ((x_{11}, x_{12}), ..., (x_{i1}, x_{i2})) \in \phi^2(P).$$

Comme f est donné par des polynômes et R admet $\wedge$, $(\mathrm{im}(f), L, \phi_f)$ est diophantien dans (R, L, ϕ).

En outre, il y a une bijection d'ensembles $(\mathrm{im}(f), L, \phi_f) = (R^2, L, \phi^2)$. $\square$

Si ce principe §6 s'applique, nous disons que (R, L) est *couvert par n fonc-*

tions de stockage. Si on peut prendre $n = 1$, R admet une fonction de stockage, propriété connue de la théorie de récursion et de l'informatique. Lew et Rosenberg [26] démontrent entre autres la non-existence de fonctions de stockage quadratiques pour $\mathbf{Z}$ (c.-à-d. telles que $n = 1$ et $\deg(f_1) = 2$). L'existence de telles fonctions (non-quadratiques) n'est pas connue. Les deux propositions suivantes peuvent être considérées comme des résultats partiels ultérieurs dans le cadre de cette question.

7. Proposition. – $(\mathbf{Z}, (0, 1, +, \cdot, =))$ *est couvert par 4 fonctions de stockage.*

Preuve. Soient $C_{>0} : \mathbf{Z}^2_{>0} \to \mathbf{Z}_{>0}$ et $C_{\geq 0} : \mathbf{Z}^2_{\geq 0} \to \mathbf{Z}_{\geq 0}$ respectivement les fonction de Cantor de $\mathbf{Z}_{>0}$ et $\mathbf{Z}_{\geq 0}$ ([27]), qui sont des bijections polynômiales. Considérons le recouvrement polynômial $\mathbf{Z}^2 \to \mathbf{Z}$ donné par

$$\begin{cases} (x,y) \mapsto 2C_{\geq 0}(x,y) & \text{si } (x,y) \in U_1 := \{x \geq 0 \wedge y \geq 0\} \\ (x,y) \mapsto -2C_{\geq 0}(-x,-y) & \text{si } (x,y) \in U_2 := \{x \leq 0 \wedge y \leq 0\} - \{(0,0)\} \\ (x,y) \mapsto 2C_{>0}(-x,y) + 1 & \text{si } (x,y) \in U_3 := \{x < 0 \wedge y > 0\} \\ (x,y) \mapsto -2C_{>0}(x,-y) + 1 & \text{si } (x,y) \in U_4 := \{x > 0 \wedge y < 0\} \end{cases}$$

Les images des différents $\{U_i\}_{i=1}^4$ sont $2\mathbf{Z}_{\geq 0}, -2\mathbf{Z}_{>0}, 2\mathbf{Z}_{>0} + 1$ and $-2\mathbf{Z}_{>0} + 1$, donc diophantiens dans $\mathbf{Z}$ (comme $\mathbf{Z}_{\geq 0}$ l'est par le théorème des quatres carrés de Lagrange, et comme $x \neq 0 \iff (x \geq 0) \wedge (-x \geq 0)$). Alors le principe du §6 s'applique. □

8. Proposition. – *Soit K le corps de fonctions d'une courbe propre lisse de genre g, irréductible sur un corps k. Soit $t \in K - k$ une fonction non-constante tel que $K/k(t)$ est séparable, et soit N_t le nombre des zéros et pôles de t. Si car$(k) = 0$, supposons en outre qu'il existe un nombre naturel impair $m > 64 \cdot (N_t + \max\{5, 2g + 3\})$ tel que K ne contient que la racine triviale d'unité d'ordre m, et tel que t n'est pas m-puissance. Alors $(K, (0, 1, t, +, \cdot, =))$ admet une fonction de stockage.*

Preuve. Si $\mathrm{car}(k) = p > 0$, choisissons $m = p$. Il suffit de démontrer que la fonction $f : (x, y) \to x^m + ty^m$ est injective, donc que les seules solutions de l'équation $A_1 + A_2 + A_3 + A_4 = 0$, où

$$A_1 = x_1^m,\ A_2 = tx_3^m,\ A_3 = -x_2^m,\ A_4 = -tx_4^m,$$

satisfont $A_1 + A_3 = 0$. Si $\mathrm{car}(k) = p$, alors le dérivé par rapport à t est une dérivation globale sur K (comme $K/k(t)$ est séparable), et en l'applicant à l'équation, le résultat est immédiat.

Supposons donc que $\mathrm{car}(k) = 0$. Paraphrasons un résultat auxiliaire de Mason ([28], Lemme 2): *Soit $n \geq 3$, et $A_1 + ... + A_n = 0$ pour $(A_1, ..., A_n) \in K^n$. Alors une sous-somme est zéro (c.-à-d. $e_1 A_1 + ... + e_n A_n = 0$, $e_i \in \{0, 1\}$ et $(\exists i)(e_i = 0)$), où l'inégalité suivante vaut:*

$$\sum_v \max\{0, -v(A_1), ..., -v(A_n)\} \leq 4^{n-2}(|S| + \max\{0, 2g - 2\}).$$

Ici, v parcourt les k-valuations discrètes normalisées inéquivalentes de K, et S est l'ensemble des valuations pour lesquelles les A_i ne sont pas des unités.

Supposons que aucune sous-somme de $A_1 + ... + A_4$ n'est zéro. Soit ∞ une place de K, tel que la valuation v_∞ correspondante satisfait $v_\infty(t) < 0$. En multipliant $x_1, ..., x_4$ avec un élément de l'anneau des fonctions régulières en dehors de ∞, nous pouvons supposer que $v(A_i) \geq 0$ pour tout $v \neq v_\infty$. Comme $\sum_v v(x) = 0$ pour tout $x \in K$, on voit que $v_\infty(A_i) \leq 0$. Dans l'inégalité du lemme (appliquée pour $n = 4$ dans notre cas), on peut remplacer la partie inférieure par $-mv_\infty(x_i)$ pour tout $i = 1, ..., 4$. On peut aussi estimer

$$|S| \leq N_t + \sum_{i, v(x_i) \neq 0} 1 \leq N_t + \sum_{i, v_\infty(x_i) \neq 0} 1 + \sum_{i, v \neq v_\infty} v(x_i) \leq N_t + 4 - v_\infty(x_1 \cdot x_2 \cdot x_3 \cdot x_4).$$

Adition des quatres inégalités obtenues donne

$$(m - 4^3)(-v_\infty(x_1 \cdot x_2 \cdot x_3 \cdot x_4)) \leq 4^3 \cdot (N_t + \max\{4, 2g + 2\}),$$

une contradiction.

Si par exemple $A_1 = 0$, on peut appliquer le lemme de Mason (pour $n = 3$) de façon analogue à $A_2 + A_3 + A_4 = 0$ pour obtenir une contradiction. Si $A_1 + A_2 = 0$ ou $A_1 + A_4 = 0$, alors $\pm t$ serait puissance d'ordre m dans K, qui est impossible (m est impair). Donc $A_1 + A_3 = 0$, c.q.f.d. □

9. *Examples.* – Un t tel que $K/K(t)$ est séparable existe si k est parfait; si $\mathrm{car}(k) = 0$ ou si $\mathrm{car}(k) = p$ et $K^p \neq K$. La proposition s'applique à tout corps de fonctions réel (c.-à-d. tel que $k \subseteq \mathbf{R}$), et à tout corps de fonctions sur la fermeture séparable d'un corps fini. Est-ce-que le résultat reste valable pour les corps de fonctions complexes, ou pour des corps de fonctions munis du langage $(0, 1, +, \cdot, \text{“} \notin k\text{”})$?

10. *Remarque.* – Le lemme de Mason est une sorte d'hypothèse ABC généralisée pour les corps de fonctions. L'hypothèse ABC généralisée (non-démontrée) pour $\mathbf{Z}$ (*cf.* Browkin et Brzezinski [23]), implique que $\mathbf{Z}$ admet $(x, y) \mapsto x^N + 2y^N$ comme fonction de stockage pour N assez grand.

Acknowledgments. The author is post-doctoral fellow of the Fund for Scientific Research - Flanders (FWO -Vlaanderen). Part of this work was done while visiting the MPIM. Thanks to Jan Van Geel for his stimulating interest.
L'auteur est Chargé de Recherches du Fonds de la Récherche Scientifique - Flandres (Belgique) (FWO). Cette note était accomplie au MPIM.

References

[1] S.B. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. A.M.S. **27** (1992), no. 1, 68–133.

[2] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen, I, II*, Math. Z. **19** (1924), 153–246, =Collected Papers, pp. 1-94.

[3] M.L. Brown, *Singular moduli and supersingular moduli of Drinfeld modules*, Invent. Math. **110** (1992), 419–439.

[4] S.D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **XVII** (1970), 255–271.

[5] G. Cornelissen, *Sur les zéros des séries d'Eisenstein de poids $q^k - 1$ pour $GL_2(\mathbf{F}_q[T])$*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), 817–820.

[6] ———, *Deligne's congruence and supersingular reduction of Drinfeld modules*, MPIM preprint 98-18.

[7] P. Lejeune-Dirichlet, *Collected works*, Chelsea Publ. New York, 1969.

[8] V.G. Drinfeld, *Elliptic modules*, Math. Sb. **94(136)** (1974), 594–627.

[9] E.-U. Gekeler, *Zur Arithmetik von Drinfeld-Moduln*, Math. Ann. **262** (1983), 167–182.

[10] ———, *Drinfeld modular curves*, Lecture Notes in Math., vol. 1231, Springer, Berlin - Heidelberg - New York, 1986.

[11] ———, *On the coefficients of Drinfeld modular forms*, Invent. Math. **93** (1988), 667–700.

[12] ———, *Some new results on modular forms for* $GL(2, \mathbf{F}_q[T])$, to appear in KAIST proceedings, 1997.

[13] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. **476** (1996), 27–93.

[14] D. Goss, *Modular forms for* $F_r[T]$, J. Reine Angew. Math. **317** (1980), 16–39.

[15] P.M. Neumann, *Some primitive permutation groups*, Proc. London Math. Soc. (3) **50** (1985), 265–281.

[16] F.K.C. Rankin and H.P.F. Swinnerton-Dyer, *On the zeros of Eisenstein series*, Bull. London Math. Soc. **2** (1970), 169–170.

[17] R.A. Rankin, *The zeros of certain Poincaré series*, Compositio Math. **46** (1982), 255–272.

[18] J.-P. Serre, *Corps locaux*, Actualités scientifiques et industrielles, vol. 1296, Hermann, Paris, 1968.

[19] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. of the Math. Soc. of Japan, vol. 11, Iwanami Shoten and Princeton University Press, 1971.

[20] P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), no. 1, 1–19.

[21] H. Wielandt, Werke, vol. I, (a) *Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad*, pp. 23-46; (b) *Finite Permutation groups*, pp. 119-198 (de Gruyter, Berlin - New York, 1994).

[22] J. Yu, *Transcendence and Drinfeld modules*, Invent. Math. **83** (1986), 507–517.

[23] J. Browkin et J. Brzeziński, *Some remarks on the abc-conjecture*, Math. Comp. **62** (1994), no. 206, 931–939.

[24] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.

[25] ———, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium '78 (Mons, 1978), Stud. Logic Foundations Math., vol. 97, North-Holland, Amsterdam, 1979, pp. 131–145.

[26] John S. Lew et Arnold L. Rosenberg, *Polynomial indexing of integer lattice-points. I. General concepts and quadratic polynomials, II. Nonexistence results for higher degree polynomials*, J. Number Theory **10** (1978), no. 2, 192–243.

[27] Yu. I. Manin, *A course in mathematical logic*, Graduate Texts in Math., vol. **54**, Springer, Berlin - Heidelberg - New York (1977).

[28] R. C. Mason, *Norm form equations I*, J. Number Theory **22** (1986), no. 2, 190-207.

[29] Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8.

Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, D-53225 Bonn *(current)*

University of Gent, Dept. of Pure Mathematics, Galglaan 2, B-9000 Gent

e-mail: `gc@cage.rug.ac.be`