

Analytic Theory of Function Fields.

Trevor D. Wooley, Fall 2024, Purdue University.

§1. Introduction to function fields.

We first need to introduce the concept of a function field as it pertains to this class. We shall need:

- (a) \mathbb{F}_p , the finite field having p elements (for prime p), which we may choose to think of as being $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$.
- (b) \mathbb{F}_q , the finite field having q elements, with $q = p^h$ for some prime p and $h \in \mathbb{N}$.

Recall that all finite fields having q elements are isomorphic to one another, so we may speak of "the" finite field of q elements.

We will make use of the standard properties of finite fields from basic courses in abstract algebra and Galois theory, though often explicitly recalling these properties. In particular, it is often useful to recall that

the units of a finite field \mathbb{F}_q , which is to say the non-zero elements \mathbb{F}_q^\times , form a multiplicative group generated by a single element (a primitive root), so

$$\mathbb{F}_q^\times = \langle c \rangle, \quad \text{for some } c \in \mathbb{F}_q^\times.$$

- (c) $\mathbb{F}_q[t]$, the ring of polynomials over the field \mathbb{F}_q ,

$$\mathbb{F}_q[t] = \left\{ \sum_{i=0}^n a_i t^i : a_i \in \mathbb{F}_q, n \geq 0 \right\}.$$

As we learn in abstract algebra, the ring $\mathbb{F}_q[t]$ is a PID (Principal Ideal Domain), and hence also a UFD (Unique Factorisation Domain). It

(2)

has the finite unit group \mathbb{F}_q^\times , and shares many properties — not just these — in common with \mathbb{Z} (the ring of integers).

This is our first analogy

Analogy 1: $\mathbb{F}_q[t] \longleftrightarrow \mathbb{Z}$.

A little experimentation reveals that a notion of positivity can be obtained by insisting that we consider lead coefficients restricted to be 1

Analogy 2: $\mathbb{F}_q[t]^+ \longleftrightarrow \mathbb{N}$
" " " "
 $\{f \in \mathbb{F}_q[t] : f \text{ monic}\} \sim \{1, 2, \dots\}$.

(d) $\mathbb{F}_q(t)$, the field of rational functions over the field \mathbb{F}_q .

This is our first example of a function field!

$\mathbb{F}_q(t) =$ field of fractions of $\mathbb{F}_q[t]$ (as defined in abstract algebra)
 $= \left\{ \frac{f}{g} : f, g \in \mathbb{F}_q[t], g \neq 0 \right\}$

Here, of course, we implicitly make use of an equivalence relation acting so that $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$ if and only if $f_1 g_2 = f_2 g_1$.

Examples of elements of $\mathbb{F}_q(t)$: $\frac{1}{t}$, $\frac{1}{t^2+2}$, $\frac{t^3+3t+2}{t+5}$, t^3+1 .

Analogy 3: $\mathbb{F}_q(t) \longleftrightarrow \mathbb{Q}$

(e) $\mathbb{F}_q((1/t))$, the field of formal Laurent series over the field \mathbb{F}_q .

This may be a new definition for the reader:

$\mathbb{F}_q((1/t)) = \left\{ \sum_{n=N}^{\infty} \frac{a_n}{t^n} : a_n \in \mathbb{F}_q, N \in \mathbb{Z} \right\}$ (Note: N may be negative!)

③

The addition and multiplication relations work in the expected way, so that when $N \geq M$, one has

$$\sum_{n=N}^{\infty} \frac{a_n}{t^n} + \sum_{m=M}^{\infty} \frac{b_m}{t^m} = \sum_{l=N}^{\infty} \frac{c_l}{t^l},$$

where

$$c_l = \begin{cases} a_l & \text{when } M < l \leq N, \\ a_l + b_l & \text{when } l \leq M. \end{cases}$$

Also,

$$\left(\sum_{n=N}^{\infty} \frac{a_n}{t^n} \right) \left(\sum_{m=M}^{\infty} \frac{b_m}{t^m} \right) = \sum_{l=N+M}^{\infty} \frac{c_l}{t^l},$$

where

$$c_l = \sum_{\substack{n \geq N \\ m \geq M \\ n+m=l}} a_n b_m.$$

One can check the field axioms for this set equipped with these definitions for addition and multiplication. In particular, if $u \in \mathbb{F}_q((1/t)) \setminus \{0\}$, then $u^{-1} \in \mathbb{F}_q((1/t)) \setminus \{0\}$. (See Problem Sheet 1).

It follows that there is a copy of $\mathbb{F}_q(t)$ (and also $\mathbb{F}_q[t]$) inside $\mathbb{F}_q((1/t))$.

Analogy 4: $\mathbb{F}_q((1/t)) \longleftrightarrow \mathbb{R}$

A justification of this analogy requires a consideration of Cauchy sequences, and the introduction of a distance function, for $\mathbb{F}_q((1/t))$.

Notions of size: We are familiar with the degree of a polynomial

$$f(t) = a_n t^n + \dots + a_1 t + a_0 \in \mathbb{F}_q[t],$$

namely $\deg(f) = \max \{ i \in \mathbb{Z}_{\geq 0} : a_i \neq 0 \}$. By convention, $\deg(0) = -\infty$.

④

A related quantity is the absolute value of $f \in \mathbb{F}_q[t]$

$$|f| = q^{\deg f} \quad (\text{with } |0| = 0).$$

Analogy 5: $|f| = q^{\deg f} \longleftrightarrow |n| \quad (n \in \mathbb{N})$

$$\begin{array}{ccc} \mathbb{A} := \mathbb{F}_q[t] & & \\ f \in \mathbb{F}_q[t] & & \\ | \mathbb{A} / f \mathbb{A} | & \longleftrightarrow & | \mathbb{Z} / n \mathbb{Z} | \end{array}$$

More generally, when $f/g \in \mathbb{F}_q(t)$, we define

$$\text{ord}(f/g) = \deg f - \deg g, \quad (\text{can be negative!})$$

and

$$|f/g| = q^{\text{ord}(f/g)} = q^{\deg f - \deg g}$$

Even more generally, when

$$\alpha = \sum_{n=N}^{\infty} \frac{a_n}{t^n} \in \mathbb{F}_q((1/t)), \quad \text{with } a_n \in \mathbb{F}_q,$$

we define

$$\text{ord}(\alpha) = \max \{-n \in \mathbb{Z} : a_n \neq 0\}$$

and

$$|\alpha| = q^{+\text{ord}(\alpha)}$$

One can check that $|\cdot|$ forms a valuation on $\mathbb{F}_q((1/t))$. Thus, we have

(i) $|\alpha| = 0$ if and only if $\alpha = 0$;

(ii) $|\alpha\beta| = |\alpha| \cdot |\beta|$, for $\alpha, \beta \in \mathbb{F}_q((1/t))$;

(iii) $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$ for $\alpha, \beta \in \mathbb{F}_q((1/t))$. [ultrametric inequality]

One can check that Cauchy sequences in $\mathbb{F}_q((1/t))$ converge to a limit

⑤ lying inside $\mathbb{F}_q((1/\epsilon))$. Moreover, one sees that $\mathbb{F}_q((1/\epsilon))$ is the completion of $\mathbb{F}_q(t)$ with respect to $|\cdot|$. This is analogous to \mathbb{R} being the completion of \mathbb{Q} with respect to the ordinary absolute value.

(f) $\mathbb{P}_q[t]$, the set of monic irreducible polynomials lying in $\mathbb{F}_q[t]$ (note the non-standard notation here!), sometimes called prime polynomials.

Analogy 6: $\pi \in \mathbb{P}_q[t] \longleftrightarrow$ prime number in \mathbb{N} .

In the classical world of \mathbb{Z} , we have the famous Prime Number Theorem first proved by Hadamard and de la Vallée Poussin in 1896:

$$\pi(x) := \sum_{\substack{p \leq x \\ p \text{ prime}}} 1 = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right).$$

In the function field world of $\mathbb{F}_q[t]$, we have Gauss' formula:

$$\sum_{\substack{\pi \in \mathbb{P}_q[t] \\ \deg(\pi) = n}} 1 = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d = \frac{q^n}{n} + O(q^{n/2}/n),$$

in which $\mu(\cdot)$ denotes the Möbius function, defined by

$$\mu(n) = \begin{cases} (-1)^k, & \text{when } n \text{ is squarefree and a product of } k \\ & \text{distinct primes,} \\ 0, & \text{when } n \text{ is not squarefree.} \end{cases}$$

Analogy 7: $\sum_{\substack{\pi \in \mathbb{P}_q[t] \\ \deg(\pi) = n}} 1 \sim \frac{q^n}{n} \longleftrightarrow \pi(x) \sim \frac{x}{\log x}$

Recall/
Note: $\left. \begin{array}{l} x \longleftrightarrow q^n \\ \log x \longleftrightarrow n \end{array} \right\} \frac{x}{\log x} \longleftrightarrow \frac{q^n}{n}$

©

We shall see a proof of the Prime Number Theorem in function fields later. In this course, our goal is to understand, generalise, and make use of these analogies, especially as they relate to phenomena in analytic number theory (and discrete harmonic analysis).

§2. Polynomial equations and inequalities in function fields.

Certain equations and inequalities are easy to investigate in $\mathbb{F}_q[t]$ by virtue of the graded structure available. We spend a little time in this section to record such results, since no analogue is readily available in the "number field" setting.

We begin with a classical result on solubility in finite fields.

Theorem 2.1. (Chevalley - Warning, 1936) Let k be a finite field of characteristic p , and suppose that $f_1, \dots, f_r \in k[x_1, \dots, x_s]$, where $\deg(f_i) = d_i$ ($1 \leq i \leq r$). Let $N(\underline{f})$ denote the number of solutions of the system of equations

$$f_i(\underline{x}) = 0 \quad (1 \leq i \leq r),$$

with $\underline{x} \in k^s$. Then, whenever $s > d_1 + \dots + d_r$, one has $p \mid N(\underline{f})$.

Proof. (Ax, 1964) Suppose that k has q elements (so that $q = p^h$ for some prime p). Then, for each $\underline{x} \in k^s$, and for $1 \leq i \leq r$, one has

$$1 - f_i(\underline{x})^{q-1} = \begin{cases} 1, & \text{when } f_i(\underline{x}) = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Notice that, implicitly in the last statement, we regard $1 - f_i(\underline{x})^{q-1}$ as an element of k . Write $\bar{N}(\underline{f})$ for the element of k

⑦ corresponding to the residue class of $N(\underline{f})$ modulo p (under the canonical mapping). Then

$$\bar{N}(\underline{f}) = \sum_{\underline{x} \in k^s} \prod_{i=1}^r (1 - f_i(\underline{x})^{q-1}). \quad (2.1)$$

On expanding the latter product, a typical term takes the shape

$$\sum_{\substack{(\alpha_1, \dots, \alpha_s) \in \mathbb{Z}_{\geq 0}^s \\ \alpha_1 + \dots + \alpha_s \leq (q-1)(d_1 + \dots + d_r)}} c(\underline{\alpha}) x_1^{\alpha_1} \dots x_s^{\alpha_s}, \quad (2.2)$$

where the $c(\underline{\alpha})$ are suitable elements of k , the precise definition of which need not detain us, save that $c(\underline{0}) = 1$ when all f_i have no constant terms.

Plainly, the term with $\underline{\alpha} = \underline{0}$ contributes to (2.1) an amount

$$c(\underline{0}) \sum_{\underline{x} \in k^s} 1 = c(\underline{0}) q^s = 0 \quad (\text{in } k).$$

Note that, since $s > d_1 + \dots + d_r$ and $\alpha_1 + \dots + \alpha_s \leq (q-1)(d_1 + \dots + d_r)$, then each s -tuple $\underline{\alpha}$ occurring in the sum (2.2) satisfies the condition that, either

(i) $\alpha_j = 0$ for some j , or

(ii) $(q-1) \nmid \alpha_j$ for some j .

Let j be any such value, and consider the sum

$$\sum_{\underline{x} \in k^s} x_1^{\alpha_1} \dots x_s^{\alpha_s} = \left(\sum_{x_j \in k} x_j^{\alpha_j} \right) \prod_{i \neq j} \sum_{x_i \in k} x_i^{\alpha_i}. \quad (2.3)$$

Recalling that there exists some generator $c \in k^\times$ with $k^\times = \langle c \rangle$, we see that

$$\sum_{x_j \in k} x_j^{\alpha_j} = \begin{cases} \sum_{l=0}^{q-2} (c^l)^{\alpha_j} = \frac{(c^{\alpha_j})^{q-1} - 1}{c^{\alpha_j} - 1} = 0, & \text{when } (q-1) \nmid \alpha_j \\ 0, & \text{when } \alpha_j = 0. \end{cases}$$

⑧

On substituting this conclusion into (2.3), and thence into (2.2) and (2.1), we conclude that $N(\underline{f}) = 0$ in k , whence $p \mid N(\underline{f})$. This completes the proof of the theorem. //

Corollary 2.2. Under the hypotheses of Theorem 2.1, if each f_i has no constant term, then $N(\underline{f}) \geq p$.

Proof. Note that $f_i(0) = 0$ ($1 \leq i \leq r$), so $N(\underline{f}) \geq 1$. But $p \mid N(\underline{f})$, and hence $N(\underline{f}) \geq p$. //

This conclusion shows that when each f_i has no constant term, and in particular, when each f_i is homogeneous of positive degree, then the system of equations $f_i(\underline{x}) = 0$ ($1 \leq i \leq r$), has a solution $\underline{x} \in k^s \setminus \{0\}$. (a non-trivial solution).

One can say more by working harder with exponential sums.

Theorem. (Katz, 1971). Let $f_1, \dots, f_r \in k[x_1, \dots, x_s]$ with k a finite field of characteristic p and cardinality q . Define

$$\mu = \left\lfloor \frac{s - (d_1 + \dots + d_r)}{\max d_i} \right\rfloor,$$

where $d_i = \deg(f_i)$. Also, denote by $N(\underline{f})$ the number of solutions of the system of equations $f_i(\underline{x}) = 0$ ($1 \leq i \leq r$), with $\underline{x} \in k^s$. Then $q^\mu \mid N(\underline{f})$.

The concept of C_i -fields. (a concept introduced by Lang in his thesis of 1952).

⑨

In this definition, and henceforth, we use the term form to refer to a homogeneous polynomial in one or more variables.

Definition 2.3. Let K be a field, and let $i \in \mathbb{Z}_{\geq 0}$. Suppose that for any form $f \in K[x_1, \dots, x_s]$ of degree d with $s > d^i$, the equation $f(\underline{x}) = 0$ has a non-trivial solution $\underline{x} \in K^s \setminus \{0\}$. Then the field K is called C_i .

It follows that a field K is C_0 if and only if K is algebraically closed. To see this, consider a binary form $g(x_1, x_2)$ lying in $K[x_1, x_2]$. The equation $g(x_1, x_2) = 0$ has a non-trivial solution provided that one of the equations $g(t, 1) = 0$ or $g(1, t) = 0$ has a solution $t \in K$, and the desired conclusion follows.

Theorem 2.4. Let k be a finite field. Then k is C_1 .

Proof. It follows from the Chevalley-Waring theorem that when $f \in k[x_1, \dots, x_s]$ is a form of degree d with $s > d$, then $f(\underline{x}) = 0$ has a non-trivial solution (see Corollary 2.2). Thus k is C_1 . //

Building on earlier work of Tsen, Lang (in his thesis of 1952) showed that:

(i) When K is a C_i field, then whenever $f_1, \dots, f_r \in K[x_1, \dots, x_s]$ are forms of degree d with $s > r d^i$, then the equations $f_i(\underline{x}) = 0$ ($1 \leq i \leq r$)

10

have a simultaneous non-trivial solution $\underline{x} \in K^s \setminus \{0\}$.

(ii) when K is a C_i field, and E is an algebraic extension of K , then E is a C_i field.

(iii) when K is a C_i field, and F is an extension of K having transcendence degree j , then F is a C_{i+j} field. In particular, when t_1, \dots, t_j are independent transcendental elements over K , then $K(t_1, \dots, t_j)$ is a C_{i+j} field.

We aim to avoid some of the complications of the Lang-Nagata approach, and seek instead a conclusion more narrowly focused on function fields.

Definition 2.5. Let K be a field, and let $i \in \mathbb{Z}_{\geq 0}$. Suppose that for any polynomials $f_1, \dots, f_r \in K[x_1, \dots, x_s]$ having no constant terms, of respective degrees d_1, \dots, d_r , and with $s > d_1^i + \dots + d_r^i$, the equations $f_1(\underline{x}) = \dots = f_r(\underline{x}) = 0$ have a non-trivial solution $\underline{x} \in K^s \setminus \{0\}$. Then the field K is called strongly C_i .

It follows from elimination theory (or algebraic geometry) that an algebraically closed field K is strongly C_0 .

Theorem 2.6. Let k be a finite field. Then k is strongly C_1 .

Proof: This follows directly from the Chevalley-Waring theorem. //

Theorem 2.7. Let K be a strongly C_i field. Then the field of rational functions $K(t)$ is a strongly C_{i+1} field.

Proof. Let $L = K(t)$, and suppose that $f_i \in L[x_1, \dots, x_s]$ is

(11)

a polynomial with no constant term of degree d_ℓ , for $1 \leq \ell \leq r$, with $s > d_1^{i+1} + \dots + d_r^{i+1}$ variables. By clearing denominators of the coefficients of f_1, \dots, f_r , we may suppose without loss of generality that each coefficient lies in $K[t]$, and has degree at most h .

We take n to be a sufficiently large positive integer, and for $1 \leq i \leq s$ we put

$$x_i = y_{i0} + y_{i1}t + \dots + y_{in}t^n, \quad (2.4)$$

where we consider the y_{ij} to be variables. Then

$$f_\ell(x) = f_{\ell,0}(y) + f_{\ell,1}(y)t + \dots + f_{\ell,d_\ell n+h}(y)t^{d_\ell n+h},$$

for suitable polynomials $f_{\ell,m}(y)$ in the $s(n+1)$ variables y_{ij} ($0 \leq j \leq n$, $1 \leq i \leq s$), all having no constant term, and having coefficients in K .

We seek a non-trivial solution $y \in K^{s(n+1)} \setminus \{0\}$ to the system of equations

$$f_{\ell,m}(y) = 0 \quad (1 \leq \ell \leq r, 0 \leq m \leq d_\ell n+h),$$

since in view of (2.4), this provides a solution $x \in K(t)^s \setminus \{0\}$ to the system of equations $f_\ell(x) = 0$ ($1 \leq \ell \leq r$). Since K is a strongly C_i field, such a solution exists provided that

$$s(n+1) > \sum_{\ell=1}^r \sum_{m=0}^{d_\ell n+h} (\deg(f_{\ell,m}))^i.$$

But $\deg(f_{\ell,m}) \leq \deg(f_\ell) = d_\ell$, so this is assured provided that

$$s(n+1) > \sum_{\ell=1}^r (d_\ell n+h) d_\ell^i = (n+1) \sum_{\ell=1}^r d_\ell^{i+1} + \sum_{\ell=1}^r (1+h-d_\ell) d_\ell^i.$$

(12)

If we take n large enough, then this condition is satisfied whenever

$$s > \sum_{l=1}^r d_l^{i+1},$$

and thus $K(t)$ is a strongly C_{i+1} field. //

Corollary 2.8. The field $\mathbb{F}_q(t)$ is a strongly C_2 field.

One can apply the same ideas to handle algebraic and more general transcendental extensions.

Theorem 2.9. Let K be a strongly C_i field, and suppose that L is an extension of K which is of transcendence degree j over K . Then L is a strongly C_{i+j} field.

Proof. If L has transcendence degree j over K , then L is algebraic over $K(t_1, \dots, t_j)$ for some elements t_1, \dots, t_j transcendental over K . Applying Theorem 2.7 inductively, we see that $K(t_1, \dots, t_j)$ is a strongly C_{i+j} field. It therefore suffices to show that whenever E is an algebraic extension of a strongly C_m field F , then E is strongly C_m .

Let E be an algebraic extension of F , and suppose that $f_l \in E[x_1, \dots, x_s]$ is a polynomial with no constant term of degree d_l , for $1 \leq l \leq r$, with $s > d_1^m + \dots + d_r^m$ variables. The coefficients of the polynomials f_l are all contained in a subfield E_0 , algebraic over F and with $[E_0:F] < \infty$. Let $\{\omega_1, \dots, \omega_n\}$ be an F -basis

(13)

for E_0 . For $1 \leq i \leq s$, we put

$$x_i = y_{i1}\omega_1 + \dots + y_{in}\omega_n, \quad (2.5)$$

where we consider the y_{ij} to be variables. Then

for suitable polynomials $f_{l,h}(y)$ in the sn variables y_{ij} ($1 \leq j \leq n, 1 \leq i \leq s$), all having no constant term, and having coefficients in F .

We seek a non-trivial solution $y \in F^{sn} \setminus \{0\}$ to the system of equations

$$f_{l,h}(y) = 0 \quad (1 \leq l \leq r, 1 \leq h \leq n),$$

noting that from (2.5), we then have a solution $\underline{x} \in E_0^s \setminus \{0\}$ to the system $f_l(\underline{x}) = 0$ ($1 \leq l \leq r$). Since F is a strongly C_m field, such a solution exists provided that

$$sn > \sum_{l=1}^r \sum_{h=1}^n \deg(f_{l,h})^m.$$

But $\deg(f_{l,h}) \leq \deg(f_l) = d_l$, so this is assured provided that

$$sn > \sum_{l=1}^r n d_l^m = n \sum_{l=1}^r d_l^m.$$

This condition is satisfied whenever $s > \sum_{l=1}^r d_l^m$, and thus E is strongly C_m . //

Thus, any algebraic extension of $\mathbb{F}_q[t_1, \dots, t_r]$ is strongly C_{r+1} . We note that whenever $f(x_1, \dots, x_s)$ is a polynomial of degree d with coefficients in $\mathbb{F}_q(t)$, having no constant term, then it has a non-trivial solution \underline{x} to $f(\underline{x}) = 0$ provided that $s > d^2$. However, it may be that fewer variables may ensure that a solution exists. Such issues can be addressed via modifications of the Hardy-Littlewood (circle) method.

We now turn to the topic of inequalities.

14

Theorem 2.10 (Dirichlet's approximation theorem).

Let $r \in \mathbb{N}$ and $\alpha \in \mathbb{F}_q((1/t))$. Then there exist unique polynomials $a, g \in \mathbb{F}_q[t]$ with g monic, $0 \leq \deg(g) \leq r$, $(a, g) = 1$, and $|g\alpha - a| < q^{-r}$.

Proof. Let

$$\alpha = \sum_{i \leq I} \alpha_i t^i = \alpha_I t^I + \alpha_{I-1} t^{I-1} + \dots \in \mathbb{F}_q((1/t)), \text{ with } \alpha_i \in \mathbb{F}_q,$$

and put

$$g = \sum_{j=0}^r g_j t^j, \text{ with } g_j \in \mathbb{F}_q. \quad (2.6)$$

Then

$$g\alpha = \sum_{l \leq I+r} c_l t^l,$$

where

$$c_l = \sum_{i \leq I} \sum_{\substack{0 \leq j \leq r \\ i+j=l}} \alpha_i g_j. \quad (2.7)$$

By applying linear algebra, the equations

$$\sum_{\substack{0 \leq j \leq r \\ l-j \leq I}} \alpha_{l-j} g_j = 0 \quad (-r \leq l \leq -1) \quad (2.8)$$

have a non-trivial solution $g \in \mathbb{F}_q^{r+1} \setminus \{0\}$. Fix any one such solution, define g via (2.6), and suppose $d = \deg(g)$. We have $g_d \neq 0$, and we may replace g by $g_d^{-1} g$ to suppose without loss of generality that g is monic.

In view of (2.8), we find from (2.7) that $c_l = 0$ for $(-r \leq l \leq -1)$.

Put $a = c_0 + c_1 t + \dots + c_{I+r} t^{I+r}$ when $I+r \geq 0$, and 0 otherwise.

Then
$$g\alpha = a + \sum_{l \leq -r-1} c_l t^l,$$

whence

$$|g\alpha - a| \leq q^{-r-1}.$$

(15)

Putting $g' = g / (g, a)$ and $a' = a / (g, a)$, we find that $|g' \alpha - a'| < q^{-r}$ with $(g', a') = 1$, giving the upper bound claimed in the statement.

It remains to establish the uniqueness of a, g subject to the hypotheses of the statement of the theorem. Suppose then that

$$|g_1 \alpha - a_1| < q^{-r} \quad \text{and} \quad |g_2 \alpha - a_2| < q^{-r},$$

with $0 \leq \deg(g_i) \leq r$, g_i monic and $(a_i, g_i) = 1$ ($i=1,2$).

Then we have

$$|g_2 a_1 - g_1 a_2| \leq \underbrace{|g_2(g_1 \alpha - a_1) - g_1(g_2 \alpha - a_2)|}_{\wedge} < q^r \cdot q^{-r} = 1.$$

$$\max\{|g_2| |g_1 \alpha - a_1|, |g_1| |g_2 \alpha - a_2|\}$$

Thus $g_2 a_1 = g_1 a_2$, and since $(a_1, g_1) = (a_2, g_2) = 1$, it follows that $g_1 = g_2$ & $a_1 = a_2$, proving uniqueness. //

Notice that the graded structure of $\mathbb{F}_q((1/t))$ allows us to reduce this Diophantine approximation problem to a problem in linear algebra. By adapting these ideas, one can prove analogous conclusions for polynomials (see HW 1). When $\theta \in \mathbb{F}_q((1/t))$, define

$$\|\theta\| = \min_{a \in \mathbb{F}_q[t]} |\theta - a|.$$

Then one can show by using ideas from this section (note especially the Chevalley-Waring theorem) that when $\alpha \in \mathbb{F}_q((1/t))$, one has

$$\min_{0 \leq \deg(n) \leq N} \|\alpha n^k\| < q^{-N/k} \quad (k \geq 1).$$

16

§ 3. The arithmetic of function fields.

We review some features of the arithmetic of the polynomial ring $A = \mathbb{F}_q[t]$, where $q = p^h$, with p prime and $h \in \mathbb{N}$.

Recall that there is a division algorithm, so given $u, v \in A$, with $v \neq 0$, there exist $g, r \in A$ with $u = gv + r$ satisfying either (a) $r = 0$ and $v \mid u$, or (b) $0 \leq \deg(r) < \deg(v)$ (with $r \neq 0$). Moreover, the polynomials g and r are uniquely defined with these properties.

This property allows us to consider congruences modulo v , for $v \in A \setminus \{0\}$, and the quotient ring

$$A/vA = \{ \bar{r} + vA : 0 \leq \deg(r) < \deg(v) \}.$$

Notice that $|A/vA| = q^{\deg(v)} = |v|$, since the representatives r of congruence classes modulo v are given by

$$r_0 + r_1 t + \dots + r_v t^v \quad \text{where } v = \deg(v) - 1.$$

Two elements $f, g \in A$ are relatively prime if no polynomial $d \in A$ with $\deg(d) \geq 1$ satisfies $d \mid f$ and $d \mid g$.

There is an analogue of the Chinese Remainder Theorem, so if $m_1, \dots, m_r \in A$ are pairwise coprime (pairwise relatively prime), and $m = m_1 \dots m_r$, then

$$A/mA \cong A/m_1A \oplus \dots \oplus A/m_rA.$$

If $x_i \in A/m_iA$ ($1 \leq i \leq r$), put $n_j = m/m_j$, $b_j \equiv n_j^{-1} \pmod{m_j}$,

$$x = n_1 b_1 x_1 + \dots + n_r b_r x_r$$

Then $x \equiv x_i \pmod{m_i}$ ($1 \leq i \leq r$).

17

Now we consider multiplicative structure.

Theorem 3.1. Let $\pi \in A$ be a prime polynomial. Then $(A/\pi A)^{\times}$ is a cyclic group having $|\pi|-1$ elements.

Proof. Observe that $A/\pi A$ is a field having $|\pi|$ elements, so that $(A/\pi A)^{\times} = \langle c \rangle$, some $c \in (A/\pi A)^{\times}$. //

In particular, if $\deg(\pi) = d$ (and π is monic irreducible) then $|(A/\pi A)^{\times}| = q^d - 1$, and for each $a \in (A/\pi A)^{\times}$, one has

$$a^{q^d - 1} \equiv 1 \pmod{\pi}. \quad (\text{analogue of Fermat's Little Theorem})$$

||

$a^{|\pi|-1}$ Moreover, there exist elements of maximal order $|\pi|-1$.

What about congruences modulo prime powers? The situation over \mathbb{Z} is quite elegant:

(a) When p is an odd prime, then $(\mathbb{Z}/p^h\mathbb{Z})^{\times}$ is cyclic, with a single generator g known as a primitive root. Moreover, a primitive root g modulo p^2 is also primitive modulo p^h for all $h \geq 2$. (and also $h=1$!)

(b) When $h = 1$ or 2 , $(\mathbb{Z}/2^h\mathbb{Z})^{\times}$ is cyclic, and when $h \geq 3$, one has $(\mathbb{Z}/2^h\mathbb{Z})^{\times} \cong (\mathbb{Z}/2) \oplus (\mathbb{Z}/2^{h-2}\mathbb{Z})$.

||

$\langle -1, 5 \rangle$

So $(\mathbb{Z}/2^h\mathbb{Z})^{\times}$ is close to being cyclic.

The situation is more complicated in the setting of $A = \mathbb{F}_q[t]$, where we recall that $q = p^h$.

Theorem 3.2. Suppose that $\pi \in A = \mathbb{F}_q[t]$ is a monic irreducible polynomial of degree d . Let $m \in \mathbb{N}$, and write l for the least positive integer with $p^l \geq m$. Then, for all $a \in (A/\pi^m A)^\times$, one has

$$a^{p^l(\pi l - 1)} \equiv 1 \pmod{\pi^m}.$$

Proof. Observe that

$$a^{\pi l - 1} \equiv 1 \pmod{\pi},$$

whence

$$a^{\pi l - 1} = 1 + \pi b,$$

for some $b \in A$. But then

$$\begin{aligned} (a^{\pi l - 1})^{p^l} &= (1 + \pi b)^{p^l} = 1 + \pi^{p^l} b^{p^l} \\ &\equiv 1 \pmod{\pi^{p^l}}. \end{aligned}$$

Since $p^l \geq m$, we have shown that

$$a^{p^l(\pi l - 1)} \equiv 1 \pmod{\pi^m}.$$

//

Were it the case that $(A/\pi^m A)^\times$ be cyclic, then there would exist $a \in (A/\pi^m A)^\times$ having the property that

$$a^{p^l(\pi l - 1)} \equiv 1 \pmod{\pi^m}$$

only when

$$l\pi l^{m-1}(\pi l - 1) \mid p^l(\pi l - 1),$$

which is to say $(p^l)^{d(m-1)} \mid p^l$, or equivalently, $l \geq hd(m-1)$.

But $p^{l-1} \leq m$, so this is possible only when

$$p^{hd(m-1)} \leq pm.$$

⑨

One can see that this allows the possibilities (a) $m=1$,
 (b) $m=2$ and $h=d=1$, or $p=2$ and $hd=2$, (c) $m=3, p=3, h=d=1$.

We note that Theorem 3.2 provides a stronger conclusion than the function field analogue of Euler's theorem. In order to state this precisely, we define the analogue of Euler's function, for $v \in A$, namely

$$\phi(v) = |v| \prod_{\pi|v} (1 - 1/|\pi|),$$

where here, and throughout, we reserve π to denote a monic irreducible element of A (a prime polynomial).

Suppose that

$$v = v_0 \pi_1^{a_1} \dots \pi_r^{a_r},$$

where $v_0 \in \mathbb{F}_q^\times$ and $a_i \in \mathbb{N}$, with π_i a prime polynomial.

Then, in view of the Chinese Remainder Theorem, we have

$$(A/vA)^\times \cong (A/\pi_1^{a_1}A)^\times \otimes \dots \otimes (A/\pi_r^{a_r}A)^\times,$$

$$\begin{aligned} \text{so } |(A/vA)^\times| &= \prod_{i=1}^r |(A/\pi_i^{a_i}A)^\times| = \prod_{i=1}^r |\pi_i|^{a_i-1} (|\pi_i|-1) \\ &= \phi(v). \end{aligned}$$

Theorem 3.3. Let $v \in A$ have degree at least 1. Then, for all $a \in (A/vA)^\times$, one has $a^{\phi(v)} \equiv 1 \pmod{v}$.

From this theorem, we have $a^{|\pi|^{m-1}(|\pi|-1)} \equiv 1 \pmod{\pi^m}$,

which as noted above is rarely as strong as Theorem 3.2.

(20)

§4. Prime polynomials.

We return to the topic of the analogue of the Prime Number Theorem in function fields:

$$\Pi_q(h) := \sum_{\substack{\pi \in \mathbb{A} \\ \deg(\pi) = h}} 1 = \frac{1}{h} \sum_{d|h} \mu\left(\frac{h}{d}\right) q^d = \frac{q^h}{h} + O\left(\frac{q^{h/2}}{h}\right).$$

There is an algebraic approach, which we do not pursue here, which begins by noting that if $\pi \in \mathbb{A}$ has degree n , then the splitting field of π over \mathbb{F}_q is isomorphic to \mathbb{F}_{q^n} . One can now apply basic Galois Theory to study subfields of \mathbb{F}_{q^n} containing \mathbb{F}_q to identify monic irreducible elements of various degrees and corresponding subfields.

We opt instead for an approach involving a zeta function.

Definition 4.1. The zeta function of $\mathbb{A} = \mathbb{F}_q[t]$ is defined for $\operatorname{Re}(s) > 1$ by the infinite series

$$\zeta_{\mathbb{A}}(s) = \sum_{\substack{u \in \mathbb{A} \\ u \text{ monic}}} |u|^{-s}.$$

Thus, we have

$$\zeta_{\mathbb{A}}(s) = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \dots = \frac{1}{1 - q^{1-s}}.$$

This function is analytic for $\operatorname{Re}(s) > 1$, and extends by analytic continuation to the whole complex plane to give a function meromorphic on \mathbb{C} except for a simple pole at $s=1$.

Putting

$$\xi_{\mathbb{A}}(s) = q^{-s} (1 - q^{-s})^{-1} \zeta_{\mathbb{A}}(s),$$

(21)

we find that

$$\zeta_{\mathbb{A}}(s) = q^{-s} (1 - q^{-s})^{-1} (1 - q^{1-s})^{-1} = (q^s - 1)^{-1} (q^{s-1} - 1)^{-1} q^{s-1} = \zeta_{\mathbb{A}}(1-s).$$

This gives an analogue of the functional equation for the classical zeta function $\zeta(s) = \zeta(1-s)$, where

$$\zeta(s) = \frac{1}{2} s(s-1) \pi^{-s/2} \Gamma(s/2) \zeta(s).$$

Euler Product: Recall that each monic polynomial can be uniquely written as a product of prime polynomials (since \mathbb{A} is a UFD). Thus, when $\text{Re}(s) > 1$, we have

$$\zeta_{\mathbb{A}}(s) = \sum_{\substack{u \in \mathbb{A} \\ u \text{ monic}}} |u|^{-s} = \prod_{\substack{\pi \in \mathbb{A} \\ \pi \text{ prime}}} \sum_{h=0}^{\infty} |\pi^h|^{-s} = \prod_{\substack{\pi \in \mathbb{A} \\ \pi \text{ prime}}} (1 - |\pi|^{-s})^{-1}.$$

Euler product representation.

We have exchanged an infinite sum for an infinite product here, and this requires some justification. Just observe that

$$\left| \sum_{\substack{u \in \mathbb{A} \\ u \text{ monic}}} |u|^{-s} - \prod_{\substack{\pi \in \mathbb{A} \\ \pi \text{ prime} \\ \deg(\pi) \leq N}} (1 - |\pi|^{-s})^{-1} \right| \leq \sum_{\substack{u \in \mathbb{A} \\ u \text{ monic} \\ \deg(u) > N}} |u|^{-s}$$

$$\leq \frac{q^{N+1}}{q^{(N+1)s}} + \dots$$

$$\leq q^{(N+1)(1-s)} (1 - q^{1-s})^{-1}$$

$\rightarrow 0$ as $N \rightarrow \infty$. \square

We are now equipped to give a simple proof of the prime number theorem in function fields.

(22)

Theorem 4.2. (Gauss, Dedekind) One has

$$\prod_q(n) := \sum_{\substack{\pi \in A \\ \deg(\pi) = n}} 1 = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

Proof. For the sake of convenience, we write $u = q^{-s}$, and then see that

$$\zeta_A(s) = \frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d},$$

by using the Euler product, and writing a_d for the number of monic irreducibles in A of degree d . Thus

$$-\log(1 - qu) = - \sum_{d=1}^{\infty} a_d \log(1 - u^d),$$

and by differentiating with respect to u ,

$$\frac{q}{1 - qu} = \sum_{d=1}^{\infty} \frac{d a_d u^{d-1}}{1 - u^d}.$$

$$\Rightarrow \sum_{n=1}^{\infty} (qu)^n = \sum_{d=1}^{\infty} d a_d \sum_{m=1}^{\infty} (u^d)^m = \sum_{n=1}^{\infty} \left(\sum_{d|n} d a_d \right) u^n \quad (\text{using } n=md)$$

Comparing coefficients of u^n , we therefore deduce that

$$\sum_{d|n} d a_d = q^n,$$

whence, by Möbius inversion,

$$n a_n = \sum_{d|n} \mu(n/d) q^d.$$

Thus, we have

$$\prod_q(n) = a_n = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d. //$$

Corollary 4.3. One has

$$\Pi_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Proof. We have

$$\Pi_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right),$$

since if $d|n$ and $1 \leq d < n$, then $d \leq n/2$. //

Notice that

$$\sum_{\substack{\pi \in \mathbb{A} \\ \deg(\pi) \leq n}} 1 = \sum_{m=0}^n \Pi_q(m) = \frac{q^n}{n} + \frac{q^{n-1}}{n-1} + \dots + 1 + O\left(\frac{q^{n/2}}{n}\right)$$

the discrete analogue of

$$\text{li}(x) = \int_2^x \frac{dt}{\log t}$$

Some basic consequences of the Prime Number Theorem:

In the classical setting (of \mathbb{Z}), one has some useful consequences of the Prime Number Theorem

$$\sum_{p \leq x} 1 \sim \frac{x}{\log x}$$

that can be derived with care:

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + o(1)$$

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \sim C \log x, \quad \text{with } C = e^\gamma \text{ and } \gamma = 0.577\dots$$

In the function field setting, one has analogues of these results, though the proofs are made easier because one sums over all polynomials of each fixed degree up to some bound. This has algebraic significance, and summing over subsets of such sets of

(24) polynomials leads to more difficult problems better resembling the classical analogue. We now illustrate these ideas.

Example 4.4. One has

$$\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg u \leq n}} \frac{1}{|u|} = \sum_{d=0}^n \frac{q^d}{q^d} = n+1$$

(Note: monic polynomials)

[Compare $\sum_{n \leq x} \frac{1}{n} \sim \log x$ with $x = q^n$].

Example 4.5. One has

$$\sum_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \leq n}} \frac{1}{|\pi|} = \sum_{d=1}^n \frac{1}{q^d} \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right) \right)$$

$$= \sum_{d=1}^n \frac{1}{d} + O\left(\sum_{d=1}^n \frac{q^{-d/2}}{d}\right)$$

$$= \log n + O(1).$$

[Compare $\sum_{p \leq x} \frac{1}{p} \sim \log \log x + O(1)$ with $x = q^n$].

Example 4.6. One has

$$-\log \left(\prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \leq n}} \left(1 - \frac{1}{|\pi|}\right) \right) = -\log \left(\prod_{d=1}^n \prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi = d}} \left(1 - \frac{1}{|\pi|}\right) \right)$$

$$= - \sum_{d=1}^n \log \left(1 - \frac{1}{q^d}\right) \cdot \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right)\right)$$

$$= \sum_{d=1}^n \left(\frac{1}{q^d} + \frac{1}{2q^{2d}} + \dots\right) \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right)\right)$$

$$= \sum_{d=1}^n \frac{1}{d} + o(1) = \log n + o(1).$$

A more careful examination here shows, in fact, that there exists a constant $C = C(q)$ having the property that

$$-\log \left(\prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \leq n}} \left(1 - \frac{1}{|\pi|} \right) \right) = \log n + C + o(1), \text{ as } n \rightarrow \infty.$$

Thus

$$\prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \leq n}} \left(1 - \frac{1}{|\pi|} \right)^{-1} \sim e^C n \quad \text{as } n \rightarrow \infty.$$

$$\left[\text{Compare } \prod_{p \leq x} \left(1 - \frac{1}{p} \right)^{-1} \sim e^\gamma \log x, \text{ with } x = q^n \right].$$

§5. Arithmetic functions and Dirichlet Series.

Definition 5.1. (a) We say that a function $f: \mathbb{F}_q[t] \setminus \{0\} \rightarrow \mathbb{C}$ is an arithmetic function.

(b) An arithmetic function f is called multiplicative if

(i) $f(a) = 1$ for all $a \in \mathbb{F}_q^*$, and

(ii) $f(uv) = f(u)f(v)$ whenever $(u, v) = 1$.

Suppose that $u \in \mathbb{F}_q[t]^*$ has prime polynomial factorisation

$$u = u_0 \pi_1^{a_1} \cdots \pi_r^{a_r},$$

with $u_0 \in \mathbb{F}_q^*$, and π_i monic irreducible, $a_i \in \mathbb{N}$. Then

$$f(u) = f(\pi_1^{a_1}) \cdots f(\pi_r^{a_r}),$$

just as in the analogous classical theory.

26

Writing $a^h \parallel b$ when $a^h \mid b$ but $a^{h+1} \nmid b$, we then have

$$f(u) = \prod_{\pi^h \parallel u} f(\pi^h)$$

as shorthand for the previous statement.

We shall usually restrict attention to arithmetic (and multiplicative) functions defined on the monic polynomials $\mathbb{F}_q[t]^+$.

Convolutions. The (Dirichlet) convolution of two arithmetic functions f and g is defined for $u \in \mathbb{F}_q[t]^+$ by defining

$$(f * g)(u) = \sum_{\substack{d \mid u \\ d \in \mathbb{F}_q[t]^+}} f(d) g(u/d).$$

Exercise: Confirm that when f and g are multiplicative functions, then so too is $f * g$.

Familiar arithmetic functions:

$$1_A(u) = \begin{cases} 1, & \text{when } u \in \mathbb{F}_q[t]^+ \end{cases} \quad (\text{multiplicative})$$

$$\tau(u) = \sum_{\substack{d \mid u \\ d \in \mathbb{F}_q[t]^+}} 1 = 1_A * 1_A(u) \quad (\text{multiplicative}).$$

$$\tau_k(u) = \underbrace{(1_A * 1_A * \dots * 1_A)}_{k\text{-fold convolution}}(u) \quad (\text{multiplicative})$$

(27)

$$\phi(u) = |u| \prod_{\pi|u} (1 - 1/|\pi|) \quad (\text{multiplicative}).$$

Note: $(\phi * 1_{\mathbb{A}})(u) = |u|$ (multiplicative).

$$\sigma(u) = \sum_{\substack{d|u \\ d \in \mathbb{F}_q[t]^+}} |d| = (1_{\mathbb{A}} * 1 \cdot 1) \quad (\text{multiplicative}).$$

$$\mu(u) = \begin{cases} (-1)^k, & \text{when } u = \pi_1 \dots \pi_k \text{ is a product of } k \text{ distinct} \\ & \text{prime polynomials.} \\ 0, & \text{otherwise.} \end{cases} \quad (\text{multiplicative})$$

$$\text{Then } (\mu * 1_{\mathbb{A}})(u) = \begin{cases} 1, & \text{when } u=1 \\ 0, & \text{otherwise.} \end{cases}$$

$$\omega(u) = \sum_{\pi|u} 1 = \text{the number of distinct prime polynomial divisors of } u$$

$$\Omega(u) = \sum_{\pi^h||u} h = \text{total number of prime divisors of } u, \text{ counted with multiplicity.}$$

Exercise: Check that $\mu(u)^2$, $2^{\omega(u)}$ and $\mu(u)^2(-1)^{\omega(u)}$ are all multiplicative functions.

Connection with Dirichlet series. Given an arithmetic function

$f: \mathbb{F}_q[t]^+ \rightarrow \mathbb{C}$, one can define the Dirichlet series

$$D_f(s) = F(s) := \sum_{u \in \mathbb{F}_q[t]^+} f(u) |u|^{-s}$$

If one has $|f(u)| \leq |u|^B$ for all $u \in \mathbb{F}_q[t]^+$, then this series converges absolutely for $\text{Re}(s) > 1 + B$.

(28)

Note: One has $D_1(s) = \sum_{u \in \mathbb{F}_q[t]^+} |u|^{-s} = \zeta_A(s)$
 " " "
 $1/(1-q^{1-s})$.

Connection with convolution: Suppose that f and g are arithmetic functions, and the associated Dirichlet series $D_f(s)$ and $D_g(s)$ both converge absolutely in the half-plane $\text{Re}(s) > \sigma_0$. Then one has

$$\begin{aligned} D_f(s) D_g(s) &= \left(\sum_{u \in \mathbb{F}_q[t]^+} f(u) |u|^{-s} \right) \left(\sum_{v \in \mathbb{F}_q[t]^+} g(v) |v|^{-s} \right) \\ &= \sum_{w \in \mathbb{F}_q[t]^+} \left(\sum_{\substack{u|w \\ u \text{ monic}}} f(u) g(w/u) \right) |w|^{-s} \\ &= \sum_{w \in \mathbb{F}_q[t]^+} (f * g)(w) \cdot |w|^{-s} = D_{f * g}(s), \end{aligned}$$

provided that $\text{Re}(s)$ is sufficiently large.

Examples:

$$D_\tau(s) = \zeta_A(s)^2, \quad \text{since } \tau = 1_A * 1_A$$

$$\zeta_A(s) D_\mu(s) = 1$$

$$\frac{\zeta_A(s-1)}{\zeta_A(s)} = D_\mu(s) \zeta_A(s-1) = D_\phi(s)$$

Exercises

The sizes of arithmetic functions and their average values:

Just as in the classical situation over \mathbb{Z} , one can apply multiplicative structure to bound multiplicative functions by

(29)

making use of prime (polynomial) factorisations. Some basic examples follows:

Theorem 5.2. Let $\varepsilon > 0$. Then there exists a positive number $C(\varepsilon)$ having the property that, whenever $u \in \mathbb{F}_q[t]^+$, one has

$$\tau(u) \leq C(\varepsilon) |u|^\varepsilon.$$

Proof. The basic observation is that, whenever

$$u = \prod_{\pi^h \parallel u} \pi^h,$$

one has

$$\tau(u) = \prod_{\pi^h \parallel u} \tau(\pi^h) = \prod_{\pi^h \parallel u} (h+1).$$

Consequently, one has

$$\frac{\tau(u)}{|u|^\varepsilon} = \prod_{\pi^h \parallel u} \frac{h+1}{|\pi|^{h\varepsilon}}.$$

Examine the function $(h+1)/q^{d h \varepsilon}$ as a function of d . One

has

$$\frac{h+1}{|\pi|^{h\varepsilon}} \leq \frac{h+1}{2^{d h \varepsilon}}.$$

Provided that $d \geq \frac{1}{\varepsilon} \frac{\log_2(h+1)}{h}$, it follows that $\frac{h+1}{|\pi|^{h\varepsilon}} \leq 1$

(with $\text{ord}(\pi) = d$). But $\frac{\log_2(h+1)}{h} \leq \frac{\log_2(1+1)}{1} = 1$, so one has

$\frac{h+1}{|\pi|^{h\varepsilon}} \leq 1$ whenever $d \geq 1/\varepsilon$. Meanwhile, for smaller values of

d , we see that $(h+1)/|\pi|^{h\varepsilon}$ achieves its maximum either at $h=1$, or (by taking logarithms and differentiating) at

(30)

the integer nearest to the solution of

$$\frac{1}{h+1} = \varepsilon \log |\pi| \Rightarrow \frac{h+1}{|\pi|^{h\varepsilon}} \leq \frac{1 + 1/(\varepsilon \log |\pi|)}{e^{(h-1)/h}} < 1 + \frac{2}{\varepsilon}.$$

Then in either case we have

$$\frac{h+1}{|\pi|^{h\varepsilon}} < 2 + 2/\varepsilon,$$

whence

$$\frac{\tau(u)}{|u|^\varepsilon} \leq \prod_{\substack{\pi^h \parallel u \\ \deg(\pi) < 1/\varepsilon}} (2 + 2/\varepsilon) \leq (2 + 2/\varepsilon)^{q^{1/\varepsilon}}.$$

Put $C(\varepsilon) = (2 + 2/\varepsilon)^{q^{1/\varepsilon}}$, and we conclude that $\tau(u) \leq C(\varepsilon)|u|^\varepsilon$.

Theorem 5.3. There is a positive constant $C=C(q)$ having the property that, whenever $u \in \mathbb{F}_q[t]^+$ has large enough degree, then

$$\phi(u) \geq C|u| / \log_q \log_q |u|.$$

Proof. We have

$$\phi(u) = |u| \prod_{\pi|u} (1 - 1/|\pi|).$$

This quantity is smallest when u is a product of the smallest possible prime polynomials. Motivated by this observation, we consider

$$\omega_n := \prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \leq n}} \pi,$$

and consider the largest natural number n such that $|\omega_n| \leq |u|$.

Observe that

(31)

$$\log_q |\mathcal{O}_n| = \sum_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \leq n}} \log_q |\pi| = \sum_{d=1}^n d \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right) \right) = \frac{q^{n+1}}{q-1} + O(q^{n/2}).$$

Thus $n = \log_q \log_q |\mathcal{O}_n| + O(1) \leq \log_q \log_q |u| + O(1)$, and we see that

$$\phi(u) \geq |u| \prod_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg \pi \leq n+1}} (1 - 1/|\pi|) \sim |u| / e^{c_1(n+1)},$$

where c_1 is the constant obtained in our analogue of Mertens' theorem.

Hence

$$\phi(u) \geq C(q) |u| / \log_q \log_q |u|,$$

for a suitable positive constant $C(q)$. //

Averages of arithmetic functions.

One can, of course, proceed by analogy with classical treatments to determine averages of arithmetic functions. Thus, for example, one may consider the average of $\tau(n)$ in a divisor sum

$$\begin{aligned} \frac{1}{x} \sum_{1 \leq n \leq x} \tau(n) &= \frac{1}{x} \sum_{1 \leq n \leq x} \sum_{d|n} 1 = \frac{1}{x} \sum_{1 \leq d \leq x} \sum_{m \leq x/d} 1 \\ &= \frac{1}{x} \sum_{1 \leq d \leq x} \left(\frac{x}{d} + O(1) \right) = x \sum_{1 \leq d \leq x} \frac{1}{d} + O(x) \\ &= x \log x + O(x). \end{aligned}$$

Indeed, one can obtain sharper conclusions by considering the ranges $1 \leq d \leq x^{1/2}$ and $d > x^{1/2}$ separately. One may imitate this approach in the function field setting, but another idea is available.

32) Example 5.4.

Observe that

$$D_t(s) = \zeta_A(s)^2 = (1 - q^{1-s})^{-2}$$

||

$$\sum_{u \in \mathbb{F}_q[t]^+} \tau(u) |u|^{-s} = \sum_{d=0}^{\infty} \left(\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u) = d}} \tau(u) \right) q^{-ds}$$

One may therefore evaluate

$$T_q(d) := \sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u) = d}} \tau(u),$$

by comparing coefficients on left and right hand sides of the above relation, noting that absolute convergence is assured for $\text{Re}(s)$ large enough.

We have (writing $w = q^{-s}$) the expansion

$$(1 - qw)^{-2} = \sum_{n=0}^{\infty} (n+1)(qw)^n \quad \left(\text{consider } \frac{d}{dw} (1 - qw)^{-1} \right).$$

Thus

$$\sum_{n=0}^{\infty} (n+1)(qw)^n = \sum_{d=0}^{\infty} T_q(d) w^d,$$

Whence

$$T_q(d) = (d+1)q^d \quad (d \geq 0).$$

Consequently,

$$\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u) \leq n}} \tau(u) = \underbrace{(n+1)q^n + nq^{n-1} + \dots + 1} ;$$

Note that this argument works so well (compared with the classical arguments) because $T_q(d)$ corresponds to an algebraic object

33

counting points in \mathbb{F}_q on a variety.

Example 5.5. Observe that with $f(u) = \varphi(u)/|u|$, one has

$$\begin{aligned} D_f(s) &= \sum_{u \in \mathbb{F}_q[t]^+} \frac{\varphi(u)}{|u|^{s+1}} = \prod_{\pi} \left(1 + \sum_{h=1}^{\infty} \frac{\varphi(\pi^h)}{|\pi|^{h(s+1)}} \right) \\ &= \prod_{\pi} \left(1 + \frac{|\pi|-1}{|\pi|} \frac{1}{|\pi|^s - 1} \right) \\ &= \prod_{\pi} \left(\frac{|\pi|^{s+1} - 1}{|\pi|^{s+1} - |\pi|} \right) = \prod_{\pi} \left(\frac{1 - |\pi|^{-1-s}}{1 - |\pi|^{-s}} \right) \\ &= \zeta_A(s) / \zeta_A(s+1). \end{aligned}$$

Write $w = q^{-s}$. Then $\zeta_A(s) = (1 - qw)^{-1}$, whence

$$D_f(s) = \frac{1-w}{1-qw},$$

and we obtain $\frac{1-w}{1-qw} = D_f(s) = \sum_{d=0}^{\infty} \left(\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u)=d}} \frac{\varphi(u)}{|u|} \right) w^{+d}$

||

$$(1-w)(1+qw+q^2w^2+\dots) = 1 + (q-1)w + (q^2-q)w^2 + \dots$$

Hence
$$\sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u)=d}} \frac{\varphi(u)}{|u|} = q^d (1 - 1/q) = q^d / \zeta_A(2).$$

This may be compared with the classical asymptotic formula

$$\sum_{1 \leq n \leq x} \frac{\varphi(n)}{n} \sim \frac{6}{\pi^2} x.$$

§ 6. Additive characters and Fourier series.

We have in mind proving an analogue of a (quantitative) version of Dirichlet's theorem concerning primes in arithmetic progression. This entails a consideration of multiplicative characters. A ~~concrete~~ approach to such matters entails a consideration of additive characters, and the associated temptation to introduce Fourier series in the function field setting.

We must first introduce an analogue of the exponential function relevant for our purposes. We suppose as usual that $q = p^h$ and consider $A = \mathbb{F}_q[t]$, so that A has characteristic p .

(a) First we define an additive character on \mathbb{F}_p . When $a \in \mathbb{F}_p$, we identify a with an element of $\{0, 1, 2, \dots, p-1\}$, and define

$$e_p(a) = e^{2\pi i a/p}.$$

Thus $e_p(\cdot): \mathbb{F}_p \longrightarrow \mathbb{C}^\times$ (the multiplicative group of complex numbers with unit modulus).

This function satisfies

$$e_p(a+b) = e_p(a) e_p(b),$$

and defines an injective homomorphism.

We also have an orthogonality relation.

Lemma 6.1. One has

$$\frac{1}{p} \sum_{u \in \mathbb{F}_p} e_p(ua) = \begin{cases} 1, & \text{when } a = 0, \\ 0, & \text{when } a \in \mathbb{F}_p \setminus \{0\}. \end{cases}$$

Proof: When $a = 0$ the desired conclusion is self-evident. Meanwhile,

35) when $a \neq 0$, the map $u \mapsto au$ permutes the elements of \mathbb{F}_p , and one sees that

$$\sum_{u \in \mathbb{F}_p} e_p(ua) = \sum_{k=0}^{p-1} e^{2\pi i k/p} = 0,$$

by summing the geometric progression.

(b) Next we extend this definition to define an additive character

$$e_q(\cdot) : \mathbb{F}_q \rightarrow \mathbb{C}^\times.$$

This involves the trace of an element $a \in \mathbb{F}_q$, which we may define via the relation

$$\text{tr}(a) = a + a^p + \dots + a^{p^{k-1}}.$$

Recall that the Galois group $\text{Gal}(\mathbb{F}_q : \mathbb{F}_p)$ is generated by

the Frobenius homomorphism $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$, $u \mapsto u^p$ (as should be

the case) the trace of a is the sum of all the Galois conjugates of a . In particular, we have $\text{tr}(a) \in \mathbb{F}_p$. We then define

$$e_q(a) = e_p(\text{tr}(a)) = e^{2\pi i \text{tr}(a)/p}.$$

We again have a homomorphism $e_q : \mathbb{F}_q \rightarrow \mathbb{C}^\times$ satisfying the property

$$e_q(a+b) = e_q(a) e_q(b),$$

by virtue of the additive property of the trace function. Moreover, we have an orthogonality relation once again.

36

Lemma 6.2. One has

$$\frac{1}{q} \sum_{u \in \mathbb{F}_q} e_q(ua) = \begin{cases} 1, & \text{when } a=0, \\ 0, & \text{when } a \in \mathbb{F}_q \setminus \{0\}. \end{cases}$$

Proof. When $a=0$, one has $e_q(ua) = 1$, and the conclusion is clear. Meanwhile, when $a \neq 0$, the map $u \mapsto au$ permutes the elements of \mathbb{F}_q , and one sees that

$$\sum_{u \in \mathbb{F}_q} e_q(ua) = \sum_{v \in \mathbb{F}_q} e_q(v) = \sum_{v \in \mathbb{F}_q} e_p(\text{tr}(v)). \quad (6.1)$$

For each $c \in \mathbb{F}_p$, the number of solutions of the equation $\text{tr}(v) = c$, which is to say

$$v + v^p + \dots + v^{p^{h-1}} = c,$$

with $v \in \mathbb{F}_q$, is at most p^{h-1} . Since every $v \in \mathbb{F}_q$ satisfies some one of these equations, for one of the p values $c \in \mathbb{F}_p$, we see that the number of solutions is precisely p^{h-1} for each $c \in \mathbb{F}_p$.

Here, we recalled that $\text{card}(\mathbb{F}_q) = p^h$. Thus

$$\sum_{v \in \mathbb{F}_q} e_p(\text{tr}(v)) = p^{h-1} \sum_{c \in \mathbb{F}_p} e_p(c) = 0.$$

The desired conclusion is now immediate from (6.1). //

(c) Finally, we extend the definition of $e_q(\cdot)$ to define an additive character on $\mathbb{F}_q((1/t))$. Here, we take the opportunity to abbreviate $\mathbb{F}_q((t))$ to \mathbb{K} and $\mathbb{F}_q((1/t))$ to \mathbb{K}_∞ .

When $\alpha \in \mathbb{K}_\infty$, say

(37)

$$\alpha = \sum_{i \in \mathbb{N}} \alpha_i t^i,$$

with $\alpha_i \in \mathbb{F}_q$ and $N \in \mathbb{Z}$, we define the residue of α to be $\text{res}(\alpha) = \alpha_{-1}$. The latter is just the coefficient of t^{-1} .

Then, we define $e: \mathbb{K}_\infty \rightarrow \mathbb{C}^\times$ by defining

$$e(\alpha) = e_q(\text{res}(\alpha)). \quad \underline{\hspace{10em}} \quad (6.2)$$

One can now define integrals of functions defined on \mathbb{K}_∞ by making use of the natural (Haar measure) defined by letting

$$\alpha + \left(\frac{1}{t}\right)^n \{ \beta \in \mathbb{K}_\infty : |\beta| < 1 \} \text{ have measure } q^{-n},$$

uniformly for $\alpha \in \mathbb{K}_\infty$. In particular, if

$$\Pi = \left\{ \sum_{i \in \mathbb{Z}} \alpha_i t^i : \alpha_i \in \mathbb{F}_q \text{ (i.e. } i \geq -1) \right\},$$

then the measure of Π is 1 and one sees that Π is the analogue of the unit interval.

Now suppose that one has a function $F: \mathbb{K}_\infty \rightarrow \mathbb{C}$. If $I \subseteq \mathbb{K}_\infty$ is a Haar-measurable set, one can define the integral

$$\int_I F(\alpha) d\alpha$$

to be equal to

$$\lim_{M \rightarrow \infty} q^{-M} \sum_{\alpha_M \in \mathbb{F}_q} \sum_{\alpha_{M-1} \in \mathbb{F}_q} \dots \sum_{\alpha_{-M} \in \mathbb{F}_q} F(\alpha_M t^M + \dots + \alpha_{-M} t^{-M}),$$

provided that this limit exists.

We have an orthogonality relation.

Lemma 6-3. One has

$$\int_{\mathbb{T}} e(u\alpha) d\alpha = \begin{cases} 0, & \text{when } u \in \mathbb{A} \setminus \{0\}, \\ 1, & \text{when } u=0. \end{cases}$$

Proof. When $u=0$, one has

$$\begin{aligned} \int_{\mathbb{T}} e(u\alpha) d\alpha &= \int_{\mathbb{T}} e(0) d\alpha = \int_{\mathbb{T}} d\alpha \\ &= \lim_{M \rightarrow \infty} q^{-M} \sum_{\alpha_{-1} \in \mathbb{F}_q} \dots \sum_{\alpha_{-M} \in \mathbb{F}_q} 1 = 1. \end{aligned}$$

$\alpha_1 t^{-1} + \dots + \alpha_{-M} t^{-M} \in M\mathbb{T} \subseteq \mathbb{T}$

Suppose, meanwhile, that $u \in \mathbb{F}_q[t] \setminus \{0\}$. Thus,

$$u = u_d t^d + \dots + u_1 t + u_0,$$

for some $u_i \in \mathbb{F}_q$ with $u_d \in \mathbb{F}_q^\times$. When $\alpha \in \mathbb{T}$, we may write

$$\alpha = \alpha_{-1} t^{-1} + \dots + \alpha_{-r} t^{-r} + \dots,$$

with $\alpha_i \in \mathbb{F}_q$, and then

$$\alpha u = \beta_{d-1} t^{d-1} + \dots + \beta_{-r} t^{-r} + \dots,$$

where

$$\beta_j = \sum_{l=0}^d \sum_{\substack{m \leq -1 \\ l+m=j}} u_l \alpha_m \quad (j \leq d-1).$$

It follows that

$$\text{res}(u\alpha) = \beta_{-1} = u_d \alpha_{-d-1} + \dots + u_0 \alpha_{-1},$$

whence

31

$$\lim_{M \rightarrow \infty} q^{-M} \sum_{\alpha_{-1} \in \mathbb{F}_q} \dots \sum_{\alpha_{-M} \in \mathbb{F}_q} e(u(\alpha_{-1}t^{-1} + \dots + \alpha_{-M}t^{-M}))$$

$$\alpha_{-1}t^{-1} + \dots + \alpha_{-M}t^{-M} + t^{-M}\pi \in \pi$$

$$= q^{-d-1} \sum_{\alpha_{-1} \in \mathbb{F}_q} \dots \sum_{\alpha_{-d-1} \in \mathbb{F}_q} e_q(u_d \alpha_{-d-1} + \dots + u_0 \alpha_{-1})$$

$$= \prod_{j=1}^{d+1} \left(q^{-1} \sum_{\alpha_{-j} \in \mathbb{F}_q} e_q(u_{j-1} \alpha_{-j}) \right)$$

$$= \begin{cases} 0, & \text{when } u_{j-1} \in \mathbb{F}_q \setminus \{0\} \text{ for some } 1 \leq j \leq d+1, \\ 1, & \text{when } u_{j-1} = 0 \text{ for all } 1 \leq j \leq d+1. \end{cases}$$

We thus conclude that

$$\int_{\pi} e(u\alpha) d\alpha = \begin{cases} 0, & \text{when } u_0, \dots, u_d \text{ are not all } 0, \\ 1, & \text{when } u_0, \dots, u_d \text{ are all } 0. \end{cases}$$

$$= \begin{cases} 0, & \text{when } u \in \mathbb{F}_q[t] \setminus \{0\}, \\ 1, & \text{when } u = 0. \end{cases}$$

This orthogonality relation enables us to develop Fourier analysis for functions defined on $K_{\infty} = \mathbb{F}_q((1/t))$, and in particular for functions defined on $K_{\infty}/A = \mathbb{F}_q((1/t))/\mathbb{F}_q[t] \cong \pi$.

Additive characters modulo g , for $g \in \mathbb{F}_q[t]^*$.

One has an orthogonality relation for the function $e(\cdot/g) : A/gA \rightarrow \mathbb{C}^*$.

(40)

Lemma 6.4. Suppose that $g \in \mathbb{F}_q[t] \setminus \{0\}$ and $u \in \mathbb{F}_q[t]$. Then

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} e\left(\frac{a}{g}u\right) = \begin{cases} 1, & \text{when } g|u, \\ 0, & \text{when } g \nmid u. \end{cases}$$

Proof. Suppose first that $g|u$. Then $u/g \in \mathbb{F}_q[t]$, and hence for each summand on the left hand side, one has

$$\frac{a}{g}u \in \mathbb{F}_q[t].$$

Then $\text{res}\left(\frac{a}{g}u\right) = 0$, whence $e\left(\frac{a}{g}u\right) = e_q(\text{res}\left(\frac{a}{g}u\right)) = e_q(0) = 1$.

We thus find that

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} e\left(\frac{a}{g}u\right) = \frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} 1 = \frac{|g|}{|g|} = 1. \quad \square$$

Now consider the situation in which $g \nmid u$. Let $d = (g, u)$, and then write $u_1 = u/d$ and $g_1 = g/d$. By considering the residues a modulo g_1 , we see that

$$\sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} e\left(\frac{a}{g}u\right) = \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} e\left(\frac{a}{g_1}u_1\right) = \frac{|g|}{|g_1|} \sum_{\substack{b \in \mathbb{F}_q[t] \\ |b| < |g_1|}} e\left(\frac{b}{g_1}u_1\right).$$

Noting that the map $b \mapsto bu_1 \pmod{g_1}$ permutes the residues modulo g_1 , since $(u_1, g_1) = 1$, we infer that

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} e\left(\frac{a}{g}u\right) = \frac{1}{|g_1|} \sum_{\substack{c \in \mathbb{F}_q[t] \\ |c| < |g_1|}} e\left(\frac{c}{g_1}u_1\right).$$

(4)

Now suppose that $g_1 = \gamma_0 + \gamma_1 t + \dots + \gamma_r t^r$, with $\gamma_r \in \mathbb{F}_q^*$ and $\gamma_i \in \mathbb{F}_q$ ($0 \leq i < r$). Then

$$\sum_{\substack{c \in \mathbb{F}_q[t] \\ |c| < |g_1|}} e\left(\frac{c}{g_1}\right) = \sum_{c_0, \dots, c_{r-1} \in \mathbb{F}_q} e\left(\frac{c_0 + c_1 t + \dots + c_{r-1} t^{r-1}}{\gamma_0 + \gamma_1 t + \dots + \gamma_r t^r}\right)$$

$$\boxed{c = c_0 + c_1 t + \dots + c_{r-1} t^{r-1}}$$

$$= \sum_{c_0, \dots, c_{r-1} \in \mathbb{F}_q} e\left(\underbrace{(c_0 + c_1 t + \dots + c_{r-1} t^{r-1}) \cdot \frac{1}{\gamma_r t^r} \left(1 + \frac{\gamma_{r-1}}{\gamma_r} \frac{1}{t} + \dots + \frac{\gamma_0}{\gamma_r t^r}\right)}_{\frac{c_{r-1}}{\gamma_r} \frac{1}{t} + \dots}\right)$$

$$= \sum_{c_0, \dots, c_{r-2} \in \mathbb{F}_q} \sum_{c_{r-1} \in \mathbb{F}_q} e_q(c_{r-1} / \gamma_r)$$

$$= 0.$$

Hence

$$\frac{1}{|g|} \sum_{\substack{a \in \mathbb{F}_q[t] \\ |a| < |g|}} e\left(\frac{a}{g} u\right) = 0 \quad \text{when } g \nmid u. \quad \square$$

Suppose now that $f: A \rightarrow \mathbb{C}$ is an arithmetic function that is periodic with period g , for some $g \in A$. Thus $f(u+g) = f(u)$ for all $u \in A$. We define the finite

Fourier transform $\hat{f}: A \rightarrow \mathbb{C}$ by means of the relation

$$\hat{f}(k) = \frac{1}{|g|} \sum_{a \text{ mod } g} f(a) e(-ka/g). \quad (6.3)$$

A Fourier representation of f is then given by applying the orthogonality relation embodied in Lemma 6.4. Thus

$$\begin{aligned}
 f(b) &= \sum_{a \bmod g} f(a) \cdot \frac{1}{|g|} \sum_{k \bmod g} e\left(\frac{k(b-a)}{g}\right) \\
 &= \sum_{k \bmod g} e\left(\frac{kb}{g}\right) \cdot \frac{1}{|g|} \sum_{a \bmod g} f(a) e\left(-\frac{ka}{g}\right),
 \end{aligned}$$

whence

$$f(b) = \sum_{k \bmod g} \hat{f}(k) e(kb/g). \quad \text{----- (6.4)}$$

Observe that we have an analogue of Parseval's identity / Plancherel's identity. Thus,

$$\begin{aligned}
 \sum_{b \bmod g} |f(b)|^2 &= \sum_{b \bmod g} \left| \sum_{k \bmod g} \hat{f}(k) e(kb/g) \right|^2 \\
 &= \sum_{b \bmod g} \sum_{k_1 \bmod g} \sum_{k_2 \bmod g} \hat{f}(k_1) \overline{\hat{f}(k_2)} e(b(k_1 - k_2)/g),
 \end{aligned}$$

so

$$\sum_{b \bmod g} |f(b)|^2 = |g| \sum_{k \bmod g} |\hat{f}(k)|^2. \quad \text{----- (6.5)}$$

Equivalently,

$$\frac{1}{|g|} \sum_{b \bmod g} |f(b)|^2 = \sum_{k \bmod g} |\hat{f}(k)|^2.$$

Similar ideas may be developed, mimicking classical Fourier theory, for functions $f: \mathbb{T} \rightarrow \mathbb{C}$ and their Fourier series.

" $\mathbb{T} \cong \mathbb{R}/\mathbb{A}$ "

§7. Multiplicative (Dirichlet) Characters.

By analogy with the classical setting (of \mathbb{Z}), we next consider characters on the multiplicative group $(A/mA)^\times$, for $m \in A$ with $\deg(m) \geq 1$.

Definition 7.1. Let $m \in A$ have positive degree. A Dirichlet character modulo m is a totally multiplicative function $\chi: A \rightarrow \mathbb{C}$, supported on the reduced residue classes a modulo m , having period m .
 [By convention, we impose $\chi(a) = 0$ for $(a, m) \neq 1$.]

Thus, if χ is a Dirichlet character modulo m , then:

$$(a) \quad \chi(a + lm) = \chi(a), \quad \text{for all } a, l \in A;$$

$$(b) \quad \chi(ab) = \chi(a)\chi(b), \quad \text{for all } a, b \in A;$$

$$(c) \quad \chi(a) \neq 0 \quad \text{if and only if } (a, m) = 1.$$

By restricting χ to reduced residues modulo m , we may interpret χ as a function of $(A/mA)^\times$ with

$$1 = \chi(1) = \chi(a^{\phi(m)}) = \chi(a)^{\phi(m)}, \quad \text{for } (a, m) = 1,$$

so that $\chi(a) \in \mathbb{C}^\times$. Thus

$$\chi: (A/mA)^\times \rightarrow \mathbb{C}^\times$$

defines a group homomorphism. Conversely, one sees that every group homomorphism from $(A/mA)^\times$ into \mathbb{C}^\times defines a Dirichlet character.

Some basic properties of Dirichlet characters modulo m :

(d) The principal character χ_0 is the character taking the value 1 on $(A/mA)^\times$.

(44)

(e) Note that every Dirichlet character χ satisfies

$$\chi(1)^2 = \chi(1), \quad \text{whence} \quad \chi(1) = 1.$$

(f) As we observed above, one has for all $a \in (A/mA)^\times$ the relation

$$\chi(a)^{\phi(m)} = \chi(a^{\phi(m)}) = \chi(1) = 1,$$

so characters take values which are $\phi(m)$ -th roots of unity.

(g) If χ_1 and χ_2 are two Dirichlet characters modulo m , then

$\chi_1 \chi_2$ is a Dirichlet character modulo m (check (a), (b), (c)).

Here, $(\chi_1 \chi_2)(a) := \chi_1(a) \chi_2(a)$ whenever $a \in (A/mA)^\times$.

(h) When χ is a Dirichlet character modulo m , then so too is

the conjugate character $\bar{\chi}$. Moreover, for each $a \in (A/mA)^\times$,

one has $1 = \chi(a) \bar{\chi}(a) = \chi \bar{\chi}(a)$, so that $\bar{\chi}$ is the multiplicative inverse of χ .

(i) The set of Dirichlet characters modulo m , which we will call

$X(m)$, forms a group under multiplication of characters.

Note that since the values of each character on $(A/mA)^\times$ are $\phi(m)$ -th roots of unity, the value set is finite, and hence $|X(m)| < \infty$.

We will prove that $|X(m)| = \phi(m) = |(A/mA)^\times|$, and give an explicit description of each of these characters.

Our argument depends on a more general treatment of characters on finite abelian groups. When G is a finite abelian group, we consider the group \hat{G} of homomorphisms $\chi: G \rightarrow \mathbb{C}^\times$. Note that if $|G| = n$,

(45)

then $\chi(g)$ is an n th root of unity for all $g \in G$.

Lemma 7.2. Suppose that G is cyclic of order n , so that $G = \langle g \rangle$ for some $g \in G$. Then \hat{G} consists of exactly n characters

$$\chi_k : G \rightarrow \mathbb{C}^\times$$

$$\chi_k(g^m) = e^{2\pi i k m / n} \quad (1 \leq k \leq n).$$

Thus $\hat{G} = \langle \chi_1 \rangle$ is cyclic.

Proof. Consider the generator g of G . Given $\chi \in \hat{G}$, we have

$$\chi(g) = e^{2\pi i k / n} \quad \text{for some } 1 \leq k \leq n. \quad \text{Then } \chi(g^m) = \chi(g)^m = e^{2\pi i k m / n},$$

which defines this character for all elements of G . In particular,

if $\chi \in \hat{G}$, then $\chi = \chi_1^m$ for some $1 \leq m \leq n$, so $\hat{G} = \langle \chi_1 \rangle$. //

Corollary 7.3. Suppose G is cyclic of order n . Then for each $\chi \in \hat{G}$, one has

$$\sum_{a \in G} \chi(a) = \begin{cases} n & , \quad \text{when } \chi = \chi_0, \\ 0 & , \quad \text{otherwise,} \end{cases}$$

and for $a \in G$, we have

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} n & , \quad \text{when } a = \text{id}, \\ 0 & , \quad \text{otherwise.} \end{cases}$$

Proof. With notation as in the lemma, we may suppose that

$\chi = \chi_1^k$ for some $1 \leq k \leq n$, whence

$$\sum_{a \in G} \chi(a) = \sum_{r=1}^n e^{2\pi i r k / n} = \begin{cases} 0 & , \quad \text{when } 1 \leq k < n, \\ n & , \quad \text{when } k = n, \end{cases}$$

and this delivers the first conclusion. For the second, we may suppose that $a = g^l$ for some $1 \leq l \leq n$, whence

$$\sum_{\chi \in \hat{G}} \chi(a) = \sum_{r=1}^n e^{2\pi i r l / n} = \begin{cases} 0 & , \quad \text{when } 1 \leq l < n, \\ 1 & , \quad \text{when } l = n, \end{cases}$$

and again we obtain the desired conclusion. //

46

Next, we address direct products of abelian groups, with an inductive strategy in mind.

Lemma 7.4 Suppose that G_1 and G_2 are finite abelian groups, and $G = G_1 \otimes G_2$, so for each $g \in G$ we have $g = (g_1, g_2)$ for some $g_i \in G_i$ ($i=1,2$).

(a) Suppose that $\chi_i \in \hat{G}_i$ ($i=1,2$). Then the function

$$\chi : G \rightarrow \mathbb{C}^\times$$

$$\chi(g) := \chi_1(g_1) \chi_2(g_2)$$

defines a character, so $\chi \in \hat{G}$.

(b) Suppose that $\chi \in \hat{G}$. Then there exist $\chi_i \in \hat{G}_i$ ($i=1,2$)

$$\text{with } \chi(g) = \chi_1(g_1) \chi_2(g_2) \quad (g = (g_1, g_2) \in G).$$

Proof. (a) is self-evident. \square

(b) We have $g = (g_1, g_2) = (g_1, id)(id, g_2)$,

$$\text{so } \chi(g) = \chi((g_1, id)) \chi((id, g_2)).$$

Then if we define

$$\chi_1(g_1) = \chi((g_1, id)) \quad \& \quad \chi_2(g_2) = \chi((id, g_2)),$$

for each $g_i \in G_i$ ($i=1,2$), then the conclusion follows. \square

This lemma shows that $\hat{G} \cong \hat{G}_1 \otimes \hat{G}_2$.

Theorem 7.5. Let G be a finite abelian group. Then $\hat{G} \cong G$.

Proof. Any finite abelian group is (by the classification theorem) isomorphic to a direct product of cyclic groups, so

$$G \cong G_1 \otimes G_2 \otimes \dots \otimes G_r,$$

for suitable cyclic groups G_i ($1 \leq i \leq r$). Now apply Lemma 7.2

(4)

and 7.4 inductively to obtain the desired conclusion. //

$$\hat{G} \cong \hat{G}_1 \otimes \hat{G}_2 \otimes \dots \otimes \hat{G}_r.$$

Corollary 7.6. One has $X(m) \cong (A/mA)^{\times}$, and, in particular $|X(m)| = \phi(m)$.

Proof. $|X(m)| = |(A/mA)^{\times}| = \phi(m)$. //

Corollary 7.7. Suppose that G is an abelian group. Then for each $\chi \in \hat{G}$, one has

$$\sum_{a \in G} \chi(a) = \begin{cases} |G|, & \text{when } \chi = \chi_0, \\ 0, & \text{otherwise,} \end{cases}$$

and for $a \in G$, we have

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} |G|, & \text{when } a = \text{id}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Use the decomposition into cyclic groups $G = G_1 \otimes \dots \otimes G_r$, and associated characters $\chi_i \in \hat{G}_i$ with $\chi \in \hat{G}$ so that $\chi = \chi_1 \dots \chi_r$.

$$\chi(g) = \chi_1(g_1) \dots \chi_r(g_r) \quad \text{when } g = (g_1, \dots, g_r).$$

Thus, making use of Corollary 7.3, we have

$$\begin{aligned} \sum_{a \in G} \chi(a) &= \left(\sum_{g_1 \in G_1} \chi_1(g_1) \right) \dots \left(\sum_{g_r \in G_r} \chi_r(g_r) \right) \\ &= \begin{cases} |G_1| \dots |G_r|, & \text{when } \chi_i = \chi_0 \quad (1 \leq i \leq r) \\ 0, & \text{when } \chi_i \neq \chi_0 \quad \text{some } 1 \leq i \leq r. \end{cases} \end{aligned}$$

Since $|G| = |G_1| \dots |G_r|$, the first conclusion follows. Similarly,

$$\sum_{\chi \in \hat{G}} \chi(g) = \left(\sum_{\chi_1 \in \hat{G}_1} \chi_1(g_1) \right) \dots \left(\sum_{\chi_r \in \hat{G}_r} \chi_r(g_r) \right)$$

(48)

$$= \begin{cases} |G_1| \cdots |G_r|, & \text{when } g_i = \text{id } (1 \leq i \leq r), \\ 0, & \text{when } g_i \neq \text{id } \text{ some } 1 \leq i \leq r, \end{cases}$$

$$= \begin{cases} |G|, & \text{when } g = (g_1, \dots, g_r) = \text{id}, \\ 0, & \text{when } g \neq \text{id}, \end{cases}$$

and again the desired conclusion follows. //

For our purposes, it is useful to record the special case given below.

Corollary 7.8. For each $\chi \in X(m)$, one has

$$\sum_{a \in (A/mA)^\times} \chi(a) = \begin{cases} \phi(m), & \text{when } \chi = \chi_0, \\ 0, & \text{otherwise.} \end{cases}$$

Also, if $a \in A$ satisfies $(a, m) = 1$, then

$$\sum_{\chi \in X(m)} \chi(a) = \begin{cases} \phi(m), & \text{when } a \equiv 1 \pmod{m}, \\ 0, & \text{otherwise.} \end{cases}$$

As previously noted, we adopt the convention that $\chi(a) = 0$ when $(a, m) \neq 1$, and thus

$$\sum_{\substack{a \in A \\ |a| < |m|}} \chi(a) = \begin{cases} \phi(m), & \text{when } \chi = \chi_0, \\ 0, & \text{otherwise,} \end{cases}$$

and for all $a \in A$,

$$\sum_{\chi \in X(m)} \chi(a) = \begin{cases} \phi(m), & \text{when } a \equiv 1 \pmod{m}, \\ 0, & \text{otherwise.} \end{cases}$$

It is not too difficult to construct the characters $\chi \in X(m)$ explicitly.

(4)

Recall that when π is a monic irreducible element of A , then

$(A/\pi A)^{\times}$ is cyclic, and

$$\{a^{|\pi|^{-1}} : a \in (A/\pi^m A)^{\times}\} \cong \underbrace{C_{p^{a_1}}}_{\langle g_1 \rangle} \otimes \cdots \otimes \underbrace{C_{p^{a_r}}}_{\langle g_r \rangle},$$

for suitable positive integers $a_i = a_i(\pi)$ ($1 \leq i \leq r = r(\pi)$), with

$$|\pi|^{m-1} = p^{a_1 + \cdots + a_r}$$

(see Theorem 3.1 and HW2, 2.1). Thus $(A/\pi^m A)^{\times}$ can be written as an internal direct product

$$(A/\pi^m A)^{\times} = \{g_0^{b_0} g_1^{b_1} \cdots g_r^{b_r} : 0 \leq b_0 < |\pi|^{-1}, 0 \leq b_j < a_j (1 \leq j \leq r)\}$$

for suitable elements g_0, \dots, g_r of $(A/\pi^m A)^{\times}$. The characters of $(A/\pi^m A)^{\times}$ therefore take the shape

$$\chi_{\underline{k}}(a) = \exp\left(2\pi i \left(\frac{k_0 b_0}{|\pi|^{-1}} + \frac{k_1 b_1}{p^{a_1}} + \cdots + \frac{k_r b_r}{p^{a_r}}\right)\right),$$

when $a = \prod_{\pi} g_0^{b_0} g_1^{b_1} \cdots g_r^{b_r}$, where $0 \leq k_0 < |\pi|^{-1}$, $0 \leq k_j < p^{a_j}$ ($1 \leq j \leq r$).

We can determine the character of $(A/uA)^{\times}$, when $u \in A$ has degree at least 1, by using the relation

$$(A/uA)^{\times} \cong \bigotimes_{\pi^m \parallel u} (A/\pi^m A)^{\times},$$

available via the Chinese Remainder Theorem. In this case, the general character of $(A/uA)^{\times}$ takes the shape

$$\chi_{\underline{k}}(a) = \exp\left(2\pi i \sum_{\pi^m \parallel u} \left(\frac{k_0 b_0}{|\pi|^{-1}} + \frac{k_1 b_1}{p^{a_1}} + \cdots + \frac{k_r b_r}{p^{a_r}}\right)\right),$$

④ When $a = \prod_{\pi^m \parallel u} g_0^{b_0} g_1^{b_1} \dots g_r^{b_r}$, in which we have adopted

the convention that throughout, $a_i = a_{i,\pi}$, $b_i = b_{i,\pi}$, $k_i = k_{i,\pi}$, $r = r_\pi$, and where

$$0 \leq k_{0,\pi} < |\pi| - 1, \quad 0 \leq k_{j,\pi} < p^{a_{j,\pi}} \quad (1 \leq j \leq r_\pi).$$

Observe in this last formula that $\chi_\pi(a)$ is indeed a character modulo u . For certainly $b_{i,\pi}$ depends only on a modulo u . Moreover, when we consider the map $b_{0,\pi} \mapsto b_{0,\pi} + (|\pi| - 1)$, $b_{j,\pi} \mapsto b_{j,\pi} + p^{a_{j,\pi}}$ ($1 \leq j \leq r_\pi$), it follows that (in the obvious sense) each $g_i^{b_i} \mapsto g_i^{b_i}$.

Finally, we observe that while totally multiplicative functions f on A having period m , and with $f(a) = 0$ whenever $(a, m) \neq 1$, are Dirichlet characters modulo m , the same is true in the absence of the condition "totally".

Theorem 7.9. Suppose that $f: A \rightarrow \mathbb{C}$ is a multiplicative function satisfying:

- (a) $f(a) = 0$ whenever $(a, m) \neq 1$, and
- (b) $f(a + lm) = f(a)$ for all $a, l \in A$.

Then f is a Dirichlet character modulo m .

Proof. We need show only that $f(ab) = f(a)f(b)$ for all $a, b \in A$. When $(ab, m) \neq 1$, one has either $(a, m) \neq 1$ or $(b, m) \neq 1$, and hence $f(ab) = 0 = f(a)f(b)$.

Now suppose that $(ab, m) = 1$, whence $(a, m) = (b, m) = 1$.

⑤ Since $(a, m) = 1$, there exists $l \in A$ with $lm \equiv 1 - b \pmod{a}$,
whence $(a, b + lm) = 1$. Hence

$$\begin{aligned} f(ab) &= f(a(b + lm)) \\ &= f(a)f(b + lm) \\ &= f(a)f(b). \end{aligned}$$

This proves the total multiplicativity of f , confirming that f is a Dirichlet character. //

§8. Prime polynomials in arithmetic progression.

We now seek an analogue of Dirichlet's Theorem on primes in arithmetic progression - first proved in the function field setting by Kornblum (as described by Landau).

Definition 8.1. Let χ be a Dirichlet character modulus m . The Dirichlet L-function associated with χ is

$$L(s, \chi) = \sum_{u \in \mathbb{F}_q[t]^+} \frac{\chi(u)}{|u|^s}.$$

By comparison with $\zeta_{\mathbb{A}}(s) = \sum_{u \in \mathbb{F}_q[t]^+} |u|^{-s}$, we see that $L(s, \chi)$ converges absolutely for $\operatorname{Re}(s) > 1$, and moreover

$$L(s, \chi) = \prod_{\pi} \left(1 - \frac{\chi(\pi)}{|\pi|^s}\right)^{-1}. \quad (\operatorname{Re}(s) > 1).$$

We therefore see, in particular, that

$$\begin{aligned} L(s, \chi_0) &= \prod_{\pi} \left(1 - \frac{\chi_0(\pi)}{|\pi|^s}\right)^{-1} \\ &= \prod_{\pi \nmid m} \left(1 - \frac{1}{|\pi|^s}\right)^{-1} = \prod_{\pi} \left(1 - \frac{1}{|\pi|^s}\right)^{-1} \cdot \prod_{\pi | m} \left(1 - \frac{1}{|\pi|^s}\right) \end{aligned}$$

⑫

Thus, the principal character χ_0 modulo m satisfies the property that

$$L(s, \chi_0) = \prod_{\pi|m} (1 - |\pi|^{-s}) \zeta_{\mathbb{A}}(s). \quad (8.1)$$

Recall that $\zeta_{\mathbb{A}}(s) = (1 - q^{1-s})^{-1}$. Then we see from (8.1) that $L(s, \chi_0)$ can be analytically continued throughout \mathbb{C} , save for a simple pole at $s=1$. (by using the corresponding analytic continuation for $\zeta_{\mathbb{A}}(s)$).

Moreover, one has $|\pi|^{-s} = q^{-ds}$, where $d = \deg(\pi)$. Then

$L(s, \chi_0)$ takes the shape

$$L(s, \chi_0) = \frac{P_k(w)}{1 - qw}, \quad (8.2)$$

where $w = q^{-s}$ and $P_k(w) \in \mathbb{Z}[w]$ has degree \leq equal to the degree of m . The situation is different for $L(s, \chi)$ when $\chi \neq \chi_0$.

[Notice: $(1 - qw) \nmid P_k(w)$].

Theorem 8.2. Let χ be a Dirichlet character modulo m with $\chi \neq \chi_0$. Write $w = q^{-s}$. Then $L(s, \chi)$ is a polynomial in w of degree at most $\deg(m) - 1$.

Proof. We have

$$L(s, \chi) = \sum_{u \in \mathbb{F}_q[t]^+} \frac{\chi(u)}{|u|^s} = \sum_{n=0}^{\infty} A(n, \chi) q^{-ns},$$

where

$$A(n, \chi) = \sum_{\substack{u \in \mathbb{F}_q[t]^+ \\ \deg(u) = n}} \chi(u).$$

When $n \geq \deg(m)$, we find that

$$A(n, \chi) = q^{n - \deg(m)} \sum_{|a| < |m|} \chi(a) = 0 \quad (\text{by orthogonality}),$$

and hence

$$L(s, \chi) = \sum_{n=0}^{\deg(m)-1} A(n, \chi) \omega^n \quad (\text{with } \omega = q^{-s}),$$

which is a polynomial of degree at most $\deg(m)-1$. //

Corollary 8.3. When χ is a non-principal Dirichlet character modulo m , the function $L(s, \chi)$ has an analytic continuation to the whole of \mathbb{C} .

The classical proof of the Prime Number Theorem (in arithmetic progressions, over \mathbb{Z}) rests on proving that $L(1, \chi) \neq 0$ for all $\chi \neq \chi_0$. We can pursue this approach also in the function field setting, with a similar dichotomy dividing real and complex characters.

Lemma 8.4. Let $m \in \mathbb{F}_q[t]^+$ have degree at least one. Then for each $\pi \nmid m$, there exist integers e_π and f_π with $e_\pi f_\pi = \phi(m)$, such that

$$\prod_{\chi \in X(m)} L(s, \chi) = \prod_{\pi \nmid m} (1 - |\pi|^{-f_\pi s})^{-e_\pi} \quad (8.3)$$

Proof. We observe that for each prime polynomial π with $\pi \nmid m$, the map

$$\begin{aligned} \nu: X(m) &\rightarrow \mathbb{C}^\times \\ \chi &\mapsto \chi(\pi) \end{aligned}$$

is a group homomorphism. Let the order of π in $(A/mA)^\times$ be f_π . Then for every $\chi \in X(m)$ one has

$$\chi(\pi)^{f_\pi} = \chi\left(\underbrace{\pi^{f_\pi}}_{1 \pmod{m}}\right) = \chi(1) = 1,$$

so that $\chi(\pi)$ is an f_π -th root of unity. We claim that there exists $\chi \in X(m)$ for which $\chi(\pi)$ is a primitive f_π -th root of unity. In order to confirm this assertion, let d be the least common multiple of the orders of the $\chi(\pi)$ as roots of unity, for $\chi \in X(m)$. Then by considering the group structure of $\nu(X(m))$, we see that there

54

exists $\chi \in X(m)$ with $\chi(\pi)$ of order d . But then, for all $\chi \in X(m)$, one has $1 = \chi(\pi)^d = \chi(\pi^d)$, so that $\pi^d \equiv 1 \pmod{m}$. Thus $f_\pi | d$, and so $d = f_\pi$.

Since for every $\chi \in X(m)$, one has that $\chi(\pi)$ is an f_π -th root of unity, and there exists $\chi_1 \in X(m)$ with $\chi_1(\pi) = \zeta_{f_\pi}$ a primitive f_π -th root of unity, we see that

$$\nu(X(m)) = \langle \chi_1(\pi) \rangle \text{ is cyclic, of order } f_\pi,$$

whence

$$|\ker(\nu)| = |X(m)| / |\nu(X(m))| = \varphi(m) / f_\pi = e_\pi, \text{ say.}$$

We thus deduce that for each prime polynomial π with $\pi \nmid m$, one has

$$\prod_{\chi \in X(m)} (1 - \chi(\pi) |\pi|^{-s})^{-1} = \prod_{j=1}^{f_\pi} (1 - \zeta_{f_\pi}^j |\pi|^{-s})^{-e_\pi} = (1 - |\pi|^{-f_\pi s})^{-e_\pi}.$$

Hence,

$$\begin{aligned} \prod_{\chi \in X(m)} L(s, \chi) &= \prod_{\pi} \prod_{\chi \in X(m)} (1 - \chi(\pi) |\pi|^{-s})^{-1} \\ &= \prod_{\pi \nmid m} \prod_{\chi \in X(m)} (1 - \chi(\pi) |\pi|^{-s})^{-1} \\ &= \prod_{\pi \nmid m} (1 - |\pi|^{-f_\pi s})^{-e_\pi}, \end{aligned}$$

It is relatively easy to show that when χ is complex (i.e. not real) then $L(s, \chi) \neq 0$.

Lemma 8.5. Suppose that χ is a complex Dirichlet character modulo m . Then $L(1, \chi) \neq 0$.

(55)

Proof. By expanding each term $(1 - |\pi|^{-f_{\pi} s})^{-e_{\pi}}$, one sees that each of these factors has the shape $\sum_{k=0}^{\infty} c_k |\pi|^{-ks}$, with $c_k = 1$ and $c_k \geq 0$. Thus

$$\prod_{\pi \neq m} (1 - |\pi|^{-f_{\pi} s})^{-e_{\pi}} = \sum_{u \in \mathbb{F}_q[t]^+} \frac{C(u)}{|u|^s},$$

for suitable coefficients $C(u) \geq 0$ with $C(1) = 1$, and thus the Dirichlet series on the right hand side of (8.3), say $D(s)$, satisfies the property that $D(s) > 1$ when s is a real number with $s > 1$.

Suppose, if possible, that χ is a complex character with $L(1, \chi) = 0$. Then by complex conjugation, we have also $L(1, \bar{\chi}) = 0$.

Then $L(s, \chi) L(s, \bar{\chi})$ has a double zero at $s=1$. In the product $\prod_{\chi \in X(m)} L(s, \chi)$, we also have the factor $L(s, \chi_0)$

which has a simple pole at $s=1$, and all other factors are analytic at $s=1$. Then $\prod_{\chi \in X(m)} L(s, \chi)$ has a zero at $s=1$, and is (recall) analytic when $s \neq 1$. But then one cannot have

$$\prod_{\chi \in X(m)} L(s, \chi) > 1 \quad \text{when } s \text{ is real with } s > 1,$$

as was proved above. We are therefore forced to conclude that $L(1, \chi) \neq 0$ for complex χ .

⑤⑥ The case of real-valued characters is more complicated.

Lemma 8.6. Suppose that $\chi \neq \chi_0$ is a real-valued Dirichlet character modulo m . Then $L(1, \chi) \neq 0$.

Proof. If χ is real-valued, then $\chi(n) = \pm 1$ whenever $(n, m) = 1$, whence $\chi^2(n) = 1$. So $\chi^2 = \chi_0$. We again seek to obtain a Dirichlet series with non-negative coefficients, on this occasion examining the function

$$\begin{aligned}
 D(s) &= \frac{L(s, \chi^2) L(s, \chi)}{L(2s, \chi^2)} = \frac{L(s, \chi_0) L(s, \chi)}{L(2s, \chi_0)} \\
 &= \prod_{\pi \nmid m} \frac{(1 - |\pi|^{-s})^{-1} (1 - \chi(\pi) |\pi|^{-s})^{-1}}{(1 - |\pi|^{-2s})^{-1}} \\
 &= \prod_{\substack{\pi \nmid m \\ \chi(\pi) = 1}} \frac{(1 - |\pi|^{-s})^{-2}}{(1 - |\pi|^{-2s})^{-1}} \cdot \prod_{\substack{\pi \nmid m \\ \chi(\pi) = -1}} \frac{(1 - |\pi|^{-s})^{-1} (1 + |\pi|^{-s})^{-1}}{(1 - |\pi|^{-2s})^{-1}} \\
 &= \prod_{\substack{\pi \nmid m \\ \chi(\pi) = 1}} \frac{1 + |\pi|^{-s}}{1 - |\pi|^{-s}} = \prod_{\substack{\pi \nmid m \\ \chi(\pi) = 1}} (1 + 2|\pi|^{-s} + 2|\pi|^{-2s} + \dots)
 \end{aligned}$$

Thus $D(s)$ is a Dirichlet series with non-negative coefficients.

It is helpful to simplify the factors $L(s, \chi_0)$ and $L(2s, \chi_0)$ in this conclusion so that we reduce the dependence on m . Observe that

$$\begin{aligned}
 \frac{L(s, \chi_0)}{L(2s, \chi_0)} &= \prod_{\pi | m} \frac{(1 - |\pi|^{-s})}{(1 - |\pi|^{-2s})} \cdot \frac{\zeta_A(s)}{\zeta_A(2s)} \\
 &= \prod_{\pi | m} (1 + |\pi|^{-s})^{-1} \cdot \frac{1 - q^{1-2s}}{1 - q^{1-s}}
 \end{aligned}$$

(57)

Thus,

$$\frac{1-q^{1-2s}}{1-q^{1-s}} L(s, \chi) = \prod_{\pi | m} (1 + |\pi|^{-s}) \cdot D(s) = \sum_{u \in \mathbb{F}_q[t]^+} \frac{a(u)}{|u|^s}, \text{ say,}$$

is a Dirichlet series with non-negative coefficients, with $a(1) = 1$.

The proof that $L(1, \chi)$ is non-zero is made easier by converting the problem into one about rational functions. To this end, put $w = q^{-s}$, and write $L(s, \chi) = P(w, \chi)$, a polynomial in w (by Theorem 8.21).

Then

$$\frac{1-qw^2}{1-qw} P(w, \chi) = \sum_{d=0}^{\infty} \left(\underbrace{\sum_{|u|=q^d} a(u)}_{A(d)} \right) w^d,$$

where $A(d)$ is non-negative for $d \geq 0$, and $A(0) = 1$. Notice that $L(s, \chi)$ converges for $\operatorname{Re}(s) > 1$, whence $\sum_{u \in \mathbb{F}_q[t]^+} \frac{a(u)}{|u|^s}$ converges for $\operatorname{Re}(s) > 1$. Consequently, one sees that $\sum_{d=0}^{\infty} A(d) w^d$ converges for $|w| < q^{-1}$.

Goal: Prove that $L(1, \chi) \neq 0$, or equivalently, that $P(q^{-1}, \chi) \neq 0$.

Suppose that $P(q^{-1}, \chi) = 0$, and seek a contradiction. Then

$$(1-qw) \mid P(w, \chi),$$

so that $\frac{1-qw^2}{1-qw} P(w, \chi)$ is a polynomial in w . Then

$\sum_{d=0}^{\infty} A(d) w^d$ is a polynomial in w with non-negative coefficients and constant term 1 with a zero at $w = 1/\sqrt{q}$. But this is impossible, because such a polynomial has no positive roots. $\#$

(58)

We conclude that $P(q^{-1}, \chi) \neq 0 \Rightarrow L(1, \chi) \neq 0.$

Theorem 8.7. When $\chi \in X(m)$ and $\chi \neq \chi_0$, one has $L(1, \chi) \neq 0.$

Proof. Just combine the conclusions of Lemmata 8.5 and 8.6.

We are now equipped to prove an analogue of Dirichlet's theorem concerning the infinitude of primes in arithmetic progressions. This will provide only weak quantitative information without further input. We begin with a definition of Dirichlet density.

Definition 8.8. Suppose that S is a set of prime polynomials in A . The Dirichlet density of S is defined to be

$$\delta(S) = \lim_{s \rightarrow 1^+} \frac{\sum_{\pi \in S} |\pi|^{-s}}{\sum_{\pi \in A} |\pi|^{-s}}$$

provided that this limit exists.

Notice that when $s > 1$, one has

$$\sum_{\pi \in S} |\pi|^{-s} < \infty \quad \text{and} \quad \sum_{\pi \in A} |\pi|^{-s} < \infty.$$

Moreover, using the analogue of the Prime Number Theorem,

$$\begin{aligned} \sum_{|\pi| \leq q^n} |\pi|^{-1} &= \sum_{d=1}^{q^n} q^{-d} \left(\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right) \right) \\ &= \log n + O(1). \end{aligned}$$

So, morally speaking, one may regard S as having Dirichlet density δ when

$$\sum_{\substack{|\pi| \leq q^n \\ \pi \in S}} |\pi|^{-1} = \delta \log n + O(1).$$

(59)

Even more heuristically, the set \mathcal{P} contains a proportion δ of the set of prime polynomials.

Goal: We aim to show that when $(a, m) = 1$, then the Dirichlet density of the set of prime polynomials π satisfying $\pi \equiv a \pmod{m}$ is $1/\phi(m)$.

We begin by connecting the quantities employed in Definition 8.8 to zeta and L-functions.

Lemma 8.9. As $s \rightarrow 1+$, one has

$$\begin{aligned} \sum_{\pi \in \mathcal{A}} |\pi|^{-s} &= \log \zeta_{\mathcal{A}}(s) + o(1) \\ &= \log \left(\frac{1}{s-1} \right) + o(1). \end{aligned}$$

Proof. Using the Euler product representation of $\zeta_{\mathcal{A}}(s)$, we have

$$\begin{aligned} \log \zeta_{\mathcal{A}}(s) &= - \sum_{\pi} \log(1 - |\pi|^{-s}) \\ &= \sum_{\pi} \sum_{k=1}^{\infty} \frac{|\pi|^{-ks}}{k} \\ &= \sum_{\pi} |\pi|^{-s} + o \left(\underbrace{\sum_{u \in \mathbb{F}_q[t]^+} |u|^{-2s}}_{=o(1)} \right) \end{aligned}$$

This confirms the first assertion of the lemma. \square

In order to establish the second assertion, observe that

$$\log \zeta_{\mathcal{A}}(s) = -\log(1 - q^{1-s}) = -\log(1 - \exp(-(s-1)\log q)).$$

(60) Thus, as $s \rightarrow 1+$, one has

$$\begin{aligned}\log \zeta_A(s) &= -\log((s-1)\log q + O((s-1)^2)) \\ &= \log\left(\frac{1}{s-1}\right) - \log \log q + O(s-1).\end{aligned}$$

This confirms the second assertion of the lemma. //

Lemma 8.10. As $s \rightarrow 1+$, one has

$$\sum_{\pi \in A} \chi(\pi) |\pi|^{-s} = \log L(s, \chi) + O(1).$$

Moreover,

$$\log L(s, \chi) = \begin{cases} \log\left(\frac{1}{s-1}\right) + O(1), & \text{when } \chi = \chi_0, \\ O(1) & \text{when } \chi \neq \chi_0. \end{cases}$$

Proof. Again, using the Euler product representation, we see that

$$\log L(s, \chi) = -\sum_{\pi} \log(1 - \chi(\pi) |\pi|^{-s}) = \sum_{\pi} \chi(\pi) |\pi|^{-s} + O(1).$$

On recalling (8.1), we see that

$$\begin{aligned}\log L(s, \chi_0) &= \log \zeta_A(s) + \sum_{\pi | m} \log(1 - |\pi|^{-s}) \\ &= \log \zeta_A(s) + O(1),\end{aligned}$$

whence

$$\log L(s, \chi_0) = \log\left(\frac{1}{s-1}\right) + O(1).$$

Meanwhile, when $\chi \neq \chi_0$, one has $L(1, \chi) \neq 0$ and $L(s, \chi)$ is analytic throughout \mathbb{C} . Thus, as $s \rightarrow 1+$, one has

$$\log L(s, \chi) = \log L(1, \chi) + O(s-1) = O(1).$$

(61) This completes the proof of the lemma.

Theorem 8.11. Suppose that $a, m \in A$ satisfy $(a, m) = 1$ and $\deg(m) \geq 1$.

Then the Dirichlet density of the set of primes

$$P_{a,m} = \{ \pi \in A : \pi \equiv a \pmod{m} \}$$

satisfies

$$\delta(P_{a,m}) = 1/\varphi(m).$$

In particular, there are infinitely many prime polynomials π with $\pi \equiv a \pmod{m}$.

Proof. We use the orthogonality of Dirichlet characters to detect the arithmetic progression a modulo m . Thus, when $s > 1$, one has

$$\sum_{\pi \in P_{a,m}} |\pi|^{-s} = \frac{1}{\varphi(m)} \sum_{\pi \in A} |\pi|^{-s} \underbrace{\sum_{\chi \in X(m)} \chi(\pi) \bar{\chi}(a)}_{= 0 \text{ unless } \pi a^{-1} \equiv 1 \pmod{m}}$$

$$= \frac{1}{\varphi(m)} \sum_{\chi \in X(m)} \bar{\chi}(a) \sum_{\pi \in A} \chi(\pi) |\pi|^{-s}$$

$$= \frac{1}{\varphi(m)} \sum_{\chi \in X(m)} \bar{\chi}(a) \left(\log L(s, \chi) + o(1) \right),$$

as $s \rightarrow 1^+$.

By applying Lemma 8.10, we see that

$$\sum_{\pi \in P_{a,m}} |\pi|^{-s} = \frac{1}{\varphi(m)} \log L(s, \chi_0) + \frac{1}{\varphi(m)} \sum_{\substack{\chi \neq \chi_0 \\ \chi \in X(m)}} \bar{\chi}(a) \log L(s, \chi) + o(1)$$

62

$$= \frac{1}{\phi(m)} \log\left(\frac{1}{s-1}\right) + O(1).$$

Thus, on recalling Lemma 8.9, we see that

$$\lim_{s \rightarrow 1^+} \frac{\sum_{\pi \in P_{a,m}} |\pi|^{-s}}{\sum_{\pi \in \mathbb{A}} |\pi|^{-s}} = \lim_{s \rightarrow 1^+} \frac{\frac{1}{\phi(m)} \log\left(\frac{1}{s-1}\right) + O(1)}{\log\left(\frac{1}{s-1}\right) + O(1)} = \frac{1}{\phi(m)}.$$

This confirms that the Dirichlet density of $P_{a,m}$ is equal to $\frac{1}{\phi(m)}$.

§9. Prime polynomials in arithmetic progressions and the Riemann Hypothesis.

We are able to sharpen the conclusion above to give an asymptotic formula comparable in strength to the Prime (polynomial) theorem.

Theorem 9.1 Whenever $a, m \in \mathbb{A}$ satisfy $(a, m) = 1$ and $\deg(m) \geq 1$, one has

$$\sum_{\substack{\pi \in \mathbb{A} \\ \pi \equiv a \pmod{m} \\ \deg(\pi) \leq N}} 1 = \frac{1}{\phi(m)} \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Compare:

$$\sum_{\substack{\pi \in \mathbb{A} \\ \deg(\pi) \leq N}} 1 = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

In order to prove this assertion, motivated by classical treatments, the natural line of attack is to investigate the logarithmic derivatives

$$\begin{aligned} \frac{L'}{L}(s, \chi) &= \frac{d}{ds} \log L(s, \chi) \\ &= \frac{d}{ds} \sum_{\pi} \log (1 - \chi(\pi) |\pi|^{-s}) \\ &= - \sum_{\pi} \frac{\log |\pi| \chi(\pi) |\pi|^{-s}}{1 - \chi(\pi) |\pi|^{-s}} \end{aligned}$$

since we obtain

$$-\frac{L'}{L}(s, \chi) = \log q \sum_{d=1}^{\infty} d \sum_{\substack{\pi \in \mathbb{F}_q[t] \\ \deg(\pi) = d}} \frac{\chi(\pi)}{|\pi|^s} + \text{lower order terms.}$$

The right hand side here is a Dirichlet series with coefficients counting the number of prime polynomials of degree d , counted with weight $d\chi(\pi)$ (compare $\sum_{p \leq x} (\log p) \chi(p)$).

We simplify matters by substituting $w = q^{-s}$, make use of our first secret weapon ($L(s, \chi) = P(w, \chi)$ is a polynomial when $\chi \neq \chi_0$), and then make use of the remarkable fact that the Riemann Hypothesis holds in function fields, owing to work of Weil, 1948.

Let us now put this sketch into better order. Let χ be a Dirichlet character modulo m . Then $L(s, \chi) = P(w, \chi)$, where $w = q^{-s}$ and P is a polynomial of degree at most $M-1$, where $M = \deg(m)$. Thus, for suitable complex numbers $\alpha_i(\chi)$ ($1 \leq i \leq M-1$), one has

$$P(w, \chi) = \prod_{i=1}^{M-1} (1 - \alpha_i(\chi) w). \tag{9.11}$$

64 Alternatively, making use of the Euler product decomposition, one has

$$\begin{aligned}
 P(w, \chi) = L(s, \chi) &= \prod_{\pi \in M} (1 - \chi(\pi) |\pi|^{-s})^{-1} \\
 &= \prod_{d=1}^{\infty} \prod_{\substack{\pi \in M \\ \deg(\pi) = d}} (1 - \chi(\pi) q^{-ds})^{-1} \\
 &= \prod_{d=1}^{\infty} \prod_{\substack{\pi \in M \\ \deg(\pi) = d}} (1 - \chi(\pi) w^d)^{-1}. \quad \text{--- (9.2)}
 \end{aligned}$$

In order to assist in computing the logarithmic derivative, assume that

$$\frac{d}{dw} \log(1 - \alpha w^d) = \frac{-d\alpha w^{d-1}}{1 - \alpha w^d} = -\frac{d}{w} \sum_{k=1}^{\infty} (\alpha w^d)^k. \quad (|w| < 1/|\alpha|)$$

Then, on recalling (9.1), we find that when $\chi \neq \chi_0$, one has

$$\begin{aligned}
 w \frac{d}{dw} \log(P(w, \chi)) &= w \frac{d}{dw} \sum_{i=1}^{M-1} \log(1 - \alpha_i(\chi) w) \\
 &= - \sum_{i=1}^{M-1} \sum_{k=1}^{\infty} (\alpha_i(\chi) w)^k \\
 &= \sum_{k=1}^{\infty} c_k(\chi) w^k,
 \end{aligned}$$

where

$$c_k(\chi) = - \sum_{i=1}^{M-1} \alpha_i(\chi)^k. \quad \text{--- (9.3)}$$

When $\chi = \chi_0$, we instead use the relation

$$L(s, \chi_0) = \prod_{\pi \in M} (1 - |\pi|^{-s}) \sum_{\mathbb{A}} \mathbb{G}(\pi).$$

Then

$$P(w, \chi_0) = \left(\prod_{\pi \in M} (1 - w^{\deg(\pi)}) \right) (1 - qw)^{-1},$$

whence

$$w \frac{d}{dw} \log(P(w, \chi_0)) = -w \frac{d}{dw} \log(1 - qw) + w \frac{d}{dw} \sum_{\pi \in M} \log(1 - w^{\deg(\pi)})$$

(65)

$$\begin{aligned}
 &= \sum_{k=1}^{\infty} q^k w^k - \sum_{\pi \neq m} \sum_{k=1}^{\infty} w^{k \deg(\pi)} \\
 &= \sum_{k=1}^{\infty} C_k(\chi_0) w^k,
 \end{aligned}$$

where

$$C_k(\chi_0) = q^k + O_m(1). \quad (9.4)$$

It is useful at this point to recall the Riemann Hypothesis for function fields over a finite field, proved in sufficient generality for our purposes by A. Weil in 1948. This shows that the roots of L -functions of the shape $P(w, \chi)$ are $\frac{1}{2}$ -integral powers of q , and in this instance $|\alpha_i(\chi)| = 1$ or \sqrt{q} for each i when $\chi \neq \chi_0$. Note that $|w| = 1/|\alpha_i(\chi)| = 1/\sqrt{q}$ corresponds to $\operatorname{Re}(s) = 1/2$ (via $w = q^{-s}$). Observe, in particular, from (9.3) that $|C_k(\chi)| \leq (M-1)q^{k/2}$ ($\chi \neq \chi_0$).

Revert now to the Euler product formulation (9.2), and proceed in like manner. We find that

$$\begin{aligned}
 w \frac{d}{dw} \log(P(w, \chi)) &= - \sum_{d=1}^{\infty} \sum_{\substack{\pi \neq m \\ \deg(\pi)=d}} w \frac{d}{dw} \log(1 - \chi(\pi) w^d) \\
 &= \sum_{d=1}^{\infty} \sum_{\deg(\pi)=d} \sum_{k=1}^{\infty} d (\chi(\pi) w^d)^k \\
 &= \sum_{n=1}^{\infty} \left(\sum_{d|n} \sum_{\deg(\pi)=d} d \chi(\pi)^{n/d} \right) w^n
 \end{aligned}$$

(66)

Comparing coefficients of power series, one sees that when $\chi \neq \chi_0$,

$$\sum_{n=1}^{\infty} c_n(\chi) w^n = \sum_{n=1}^{\infty} \left(\sum_{d|n} \sum_{\deg(\pi)=d} d \chi(\pi)^{n/d} \right) w^n,$$

whence

$$\begin{aligned} c_n(\chi) &= \sum_{d|n} \sum_{\deg(\pi)=d} d \chi(\pi)^{n/d} \\ &= n \sum_{\deg(\pi)=n} \chi(\pi) + O\left(\sum_{d \leq n/2} d \cdot q^{d/d} \right). \end{aligned}$$

Thus

$$\begin{aligned} n \sum_{\deg(\pi)=n} \chi(\pi) &= c_n(\chi) + O(q^{n/2}) \\ &= O(q^{n/2}). \end{aligned}$$

Meanwhile, in the case $\chi = \chi_0$, we have

$$\begin{aligned} n \sum_{\deg(\pi)=n} \chi_0(\pi) &= c_n(\chi_0) + O(q^{n/2}) \\ &= q^n + O(q^{n/2}). \end{aligned}$$

Thus, when $(a, m) = 1$, we find that

$$\begin{aligned} \sum_{\substack{\deg(\pi)=n \\ \pi \equiv a \pmod{m}}} 1 &= \sum_{\deg(\pi)=n} \frac{1}{\phi(m)} \sum_{\chi \in X(m)} \chi(\pi) \bar{\chi}(a) \\ &= \frac{1}{\phi(m)} \sum_{\chi \in X(m)} \bar{\chi}(a) \sum_{\deg(\pi)=n} \chi(\pi) \\ &= \frac{1}{\phi(m)} \left(\underbrace{\frac{1}{n} (q^n + O(q^{n/2}))}_{\chi = \chi_0} + \frac{1}{n} \sum_{\chi \neq \chi_0} O_m(q^{n/2}) \right). \end{aligned}$$

(67)

We therefore conclude that

$$\sum_{\substack{\deg(\pi)=n \\ \pi \equiv a \pmod{m}}} 1 = \frac{1}{\phi(m)} \left(\frac{q^n}{n} + O_n \left(\frac{q^{n/2}}{n} \right) \right).$$

This completes the proof of Theorem 9.1. //

Before leaving this section, we provide an application of Theorem 9.1 of which we have use later on.

Theorem 9.2. Suppose that $a, g \in \mathbb{F}_q[t]$ with g monic and $(a, g) = 1$. Then one has

$$\sum_{|\pi| \leq q^N} e\left(\frac{a}{g} \pi\right) = \frac{\mu(g)}{\phi(g)} \frac{q^N}{N} + O_g\left(\frac{q^{N/2}}{N}\right).$$

Proof. We break the sum on the left hand side into arithmetic progressions modulo g . Thus, one has

$$\sum_{|\pi| \leq q^N} e\left(\frac{a}{g} \pi\right) = \sum_{\substack{|\tau| < |g| \\ (r, g) = 1}} \sum_{\substack{\pi \equiv \tau \pmod{g} \\ |\pi| \leq q^N}} e\left(\frac{a\pi}{g}\right) + O_g(1)$$

\uparrow
 accounts for π with $\pi|g$.

Note the condition $(r, g) = 1$ coming from the irreducibility of π .

Thus,

$$\sum_{|\pi| \leq q^N} e\left(\frac{a}{g} \pi\right) = \sum_{\substack{|\tau| < |g| \\ (r, g) = 1}} e\left(\frac{a\tau}{g}\right) \sum_{\substack{\pi \equiv \tau \pmod{g} \\ |\pi| \leq q^N}} 1 + O_g(1).$$

$$\begin{aligned}
&= \sum_{\substack{|r| < |g| \\ (r, g) = 1}} e\left(\frac{ar}{g}\right) \cdot \left(\frac{1}{\phi(g)} \frac{q^N}{N} + O_g\left(\frac{q^{N/2}}{N}\right) \right) + o_g(1) \\
&= \frac{1}{\phi(g)} \frac{q^N}{N} \sum_{\substack{|r| < |g| \\ (r, g) = 1}} e(ar/g) + O_g\left(\frac{q^{N/2}}{N}\right).
\end{aligned}$$

We now make use of our formula for Ramanujan's sum (in the function field setting) from Problem Set 3, Q6. Thus

$$\begin{aligned}
\sum_{\substack{|r| < |g| \\ (r, g) = 1}} e(ar/g) &= \frac{\mu(g/(g, a))}{\phi(g/(g, a))} \cdot \phi(g) \\
&= \mu(g), \quad \text{since } (g, a) = 1.
\end{aligned}$$

Then

$$\sum_{|\pi| \leq q^N} e\left(\frac{a}{g} \pi\right) = \frac{\mu(g)}{\phi(g)} \frac{q^N}{N} + O_g\left(\frac{q^{N/2}}{N}\right).$$

§10. Equidistribution: uniform distribution in function fields.

As an analogue of the unit interval $[0, 1)$ considered as the additive group \mathbb{R}/\mathbb{Z} , define

$$\mathbb{T} = \mathbb{F}_q((1/t)) / \mathbb{F}_q[t] = K_\infty / \mathbb{A},$$

and recall that we write

$$\{\alpha\} = \alpha - L\alpha,$$

where $L\alpha$ is the polynomial part of α . Thus, we have $\{\alpha\} \in \mathbb{T}$,

and one can consider \mathbb{T} to be the analogue of the unit interval $[0, 1)$, or indeed \mathbb{R}/\mathbb{Z} . Notice that, with respect to the Haar measure introduced earlier, one has

$$\text{mes}(\mathbb{T}) = \int_{\mathbb{T}} d\alpha = 1.$$

We now define analogues of intervals in \mathbb{T} . When $N \in \mathbb{N}$, we fix $I = (c_1, \dots, c_N) \in \mathbb{F}_q^N$, and then put

$$\mathcal{C}_I = \left\{ \sum_{i \leq -1} a_i t^i \in \mathbb{T} : a_i = c_{-i} \ (-N \leq i \leq -1) \right\}.$$

Thus, the cylinder set \mathcal{C}_I satisfies

$$\text{mes}(\mathcal{C}_I) = \underbrace{q^{-N}}_{\sim}$$

Definition 10.1 (Carlitz, 1952) Let $(a_x)_{x \in \mathbb{F}_q[t]}$ be a sequence of elements $a_x \in \mathbb{F}_q((1/t))$. We say that $(a_x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in \mathbb{T} if, for any cylinder set $\mathcal{C} \subseteq \mathbb{T}$, we have

$$\lim_{N \rightarrow \infty} q^{-N} \text{card} \left\{ x \in \mathbb{F}_q[t]_{\deg \leq N} : \{a_x\} \in \mathcal{C} \right\} = \text{mes}(\mathcal{C}).$$

Theorem 10.2. Suppose that $F: \mathbb{T} \rightarrow \mathbb{C}$ is integrable. Then

$$\lim_{M \rightarrow \infty} \frac{1}{M} \sum_{\substack{m \in \mathbb{F}_q[t] \\ \deg(m) < M}} F(a_m) = \int_{\mathbb{T}} F(\alpha) d\alpha$$

for all equidistributed sequences $(a_x)_{x \in \mathbb{F}_q[t]}$.

Proof. This is an exercise in basic analysis. //

We now establish an analogue for Weyl's criterion for equidistribution.

Lemma 10.3. The sequence $(a_x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in \mathbb{T} if and only if, for all $h \in \mathbb{F}_q[t] \setminus \{0\}$, one has

$$\lim_{M \rightarrow \infty} q^{-M} \left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) \leq M}} e(h a_x) \right| = 0. \quad (10.1)$$

Proof. We first show that the validity of (10.1) implies that (a_x) is equidistributed in \mathbb{T} . Let \mathcal{C} be a cylinder set, so that for some natural number N , one has

$$\mathcal{C} = \left[\beta + t^{-N} \mathbb{T} \right],$$

where $\beta = c_{+1} t^{-1} + \dots + c_{+N} t^{-N}$, for some fixed $c_1, \dots, c_N \in \mathbb{F}_q$.

Given $\varepsilon > 0$, the validity of (10.1) shows that for $M \geq M(\varepsilon, h)$, one has

$$\left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) \leq M}} e(h a_x) \right| < \varepsilon q^M.$$

Thus, for each fixed $k \in \mathbb{N}$, we have

$$\sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \beta)) = q^M + \sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \beta)),$$

whence for $M \geq M'(\varepsilon, k)$, one has

$$\left| \sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h(a_x - \beta)) - q^M \right| \leq q^k \max_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \deg(h) < k}} \left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(h a_x) \right|$$

(71)

$$< \varepsilon q^{k+M}.$$

On the other hand, by HW3, Q34, one has

$$\sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} e(h(a_x - \beta)) = \begin{cases} q^k, & \text{when } \|a_x - \beta\| < q^{-k}, \\ 0, & \text{when } \|a_x - \beta\| \geq q^{-k}. \end{cases}$$

Thus, on writing $N_k(M)$ for the number of a_x with $x \in \mathbb{F}_q[t]$ and $\deg(x) < M$ for which $\|a_x - \beta\| < q^{-k}$, we have

$$\sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} \sum_{\substack{h \in \mathbb{F}_q[t] \\ \deg(h) < k}} e(h(a_x - \beta)) = q^k N_k(M).$$

Combining these conclusions, we see that

$$|q^k N_k(M) - q^M| < \varepsilon q^{k+M}$$

$$\Rightarrow |q^{-M} N_k(M) - q^{-k}| < \varepsilon.$$

Now take $k = N$. We see that

$$|q^{-M} \text{card} \{x \in \mathbb{F}_q[t]_{\deg < M} : \{a_x\} \in \mathcal{C}\} - \text{mes}(\mathcal{C})| < \varepsilon.$$

Since this relation holds for any $\varepsilon > 0$, we conclude that

$$\lim_{M \rightarrow \infty} q^{-M} \text{card} \{x \in \mathbb{F}_q[t]_{\deg < M} : \{a_x\} \in \mathcal{C}\} = \text{mes}(\mathcal{C}),$$

and hence (a_x) is equidistributed in \mathbb{T} . \square

In the other direction, if (a_x) is equidistributed in \mathbb{T} , then

for any cylinder set $\mathcal{C} = \beta + t^{-N}\mathbb{T}$, and any $\varepsilon > 0$,

(72)

there exists $M_0 = M_0(\varepsilon, \mathcal{C})$ such that whenever $M \geq M_0(\varepsilon, \mathcal{C})$,

$$|q^{-M} \text{card} \{ x \in \mathbb{F}_q[t]_{\text{deg} < M} : \{a_x\} \in \mathcal{C} \} - \text{mes}(\mathcal{C})| < \varepsilon.$$

It follows as in the first case that with $k=N$, one has

$$|q^k N_k(M) - q^M| < \varepsilon q^{k+M},$$

and hence

$$\left| \sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \text{deg}(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \text{deg}(x) < M}} e(h(a_x - \beta)) \right| < \varepsilon q^{k+M}.$$

This shows that (take $\beta = l/t^k$ and sum over l), for any $g \in \mathbb{F}_q[t]$, when $M \geq M'_0(\varepsilon, k)$,

$$\left| \sum_{\substack{l \in \mathbb{F}_q[t] \\ \text{deg}(l) < k}} e(g l/t^k) \sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \text{deg}(h) < k}} \sum_{\substack{x \in \mathbb{F}_q[t] \\ \text{deg}(x) < M}} e(h(a_x - l/t^k)) \right| < \varepsilon q^{2k+M}$$

$$\sum_{\substack{h \in \mathbb{F}_q[t] \setminus \{0\} \\ \text{deg}(h) < k}} \left(\sum_{\substack{l \in \mathbb{F}_q[t] \\ \text{deg}(l) < k}} e(l(g-h)/t^k) \right) \sum_{\substack{x \in \mathbb{F}_q[t] \\ \text{deg}(x) < M}} e(h a_x)$$

$$\begin{cases} q^k, & \text{when } g \equiv h \pmod{t^k} \\ 0, & \text{when } g \not\equiv h \pmod{t^k}. \end{cases}$$

Thus, for each $g \in \mathbb{F}_q[t]$ with $\text{deg}(g) < k$, one finds that

$$\left| q^k \sum_{\substack{x \in \mathbb{F}_q[t] \\ \text{deg}(x) < M}} e(g a_x) \right| < \varepsilon q^{2k+M},$$

(73)

whence

$$\left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(g a_x) \right| < (\varepsilon q^k) q^M,$$

which is to say that

$$\limsup_{M \rightarrow \infty} q^{-M} \left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(g a_x) \right| < \varepsilon q^k.$$

Since $\varepsilon > 0$ is arbitrary, it follows that for every $g \in \mathbb{F}_q[t] \setminus \{0\}$, one has

$$\lim_{M \rightarrow \infty} q^{-M} \left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < M}} e(g a_x) \right| = 0.$$

□

An immediate application of Weyl's inequality shows that the sequence $(\theta x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in \mathbb{T} whenever θ is irrational.

Theorem 10.4. Suppose that $\theta \in \mathbb{K}_\infty$ is irrational. Then $(\theta x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in \mathbb{T} .

Proof. Suppose that $\theta \in \mathbb{K}_\infty$ is irrational. Then, for any $h \in \mathbb{F}_q[t] \setminus \{0\}$, one sees that $\alpha := h\theta$ is also an irrational element of \mathbb{K}_∞ . But if $\text{ord} \{h\theta\} = -N$, we find that whenever $N > M$ one has

$$\sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < N}} e(h\theta x) = \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < N}} e(\alpha x) = \begin{cases} q^N, & \text{when } \|\alpha\| < q^{-N}, \\ 0, & \text{when } \|\alpha\| \geq q^{-N}, \end{cases}$$

= 0, since ||h\theta|| = q^{-M} > q^{-N}

We therefore conclude that, for each h in F_q[t] \ {0}, one has

lim_{N -> infinity} q^{-N} | sum_{x in F_q[t], deg(x) < N} e(h(theta x)) | = 0,

which ensures that (theta x)_{x in F_q[t]} is equidistributed in T.

As we shall see, this conclusion generalises to polynomials

theta_k x^k + theta_{k-1} x^{k-1} + ... + theta_1 x,

provided that one at least of the coefficients theta_i is irrational, so long as we are not too ambitious concerning the degree k of the leading order term. To see that problems may occur when k >= p, we provide an example of Golitz (1952).

Example 10.5. When alpha = sum_{i <= n} alpha_i t^i in K_infinity, consider the map defined by

T(alpha) = alpha_{-1} t^{-1} + alpha_{-p-1} t^{-2} + alpha_{-2p-1} t^{-3} + ...

Then T is a linear map from K_infinity to T. Let

B = { alpha in K_infinity : alpha_{-1} = alpha_{-p-1} = ... = alpha_{-rp-1} = ... = 0 }

Then a countability argument shows that there exists an irrational element alpha in K_infinity with T(alpha) = 0 (i.e. alpha in B).

Given such an irrational element alpha in B, it follows that

whenever x in F_q[t], say x = sum_{i=0}^m x_i t^i, the coefficient of t^{-1}

75

in αx^p is equal to

$$\text{res}(\alpha (x_0^p + x_1^p t^1 + \dots + x_m^p t^{mp})) = \alpha_{-1} x_0^p + \alpha_{-p-1} x_1^p + \dots + \alpha_{-mp-1} x_m^p = 0.$$

Hence, the sequence $(\alpha x^p)_{x \in \mathbb{F}_q[t]}$ has the property that

$$|\{\alpha x^p\}| \leq q^{-2} \text{ for every } x \in \mathbb{F}_q[t]. \text{ In particular, one sees that}$$

the cylinder $\frac{1}{t} + t^{-N} \pi$ contains no points of the sequence (αx^p) .

modulo 1 whenever $N \geq 1$. This contradicts equidistribution in π ,

and thus $(\alpha x^p)_{x \in \mathbb{F}_q[t]}$ is not equidistributed in π for any

(irrational) element $\alpha \in \mathcal{B}$.

§11. Equidistribution: Weyl's inequality.

In order to investigate the equidistribution of polynomials $\alpha_k x^k + \dots + \alpha_1 x$ of degree $k > 1$, we shall need a version of Weyl's inequality. The idea here is to estimate the exponential sum

$$f(\alpha) = \sum_{\deg(x) < X} e(\alpha_k x^k + \dots + \alpha_1 x)$$

by repeated application of Cauchy's inequality. Thus

$$\begin{aligned} |f(\alpha)|^2 &= f(\alpha) f(-\alpha) \\ &= \sum_{\deg(x) < X} \sum_{\deg(y) < X} e((\alpha_k x^k + \dots + \alpha_1 x) - (\alpha_k y^k + \dots + \alpha_1 y)) \\ &= \sum_{\deg(h) < X} \sum_{\substack{\deg(x) < X \\ y = x+h}} e((\alpha_k((x+h)^k - x^k) + \dots + \alpha_1 h)) \end{aligned}$$

76

Notice that since $(x+h)^j - x^j = jhx^{j-1} + \dots$, it follows that the argument here may be treated as a polynomial of degree $k-1$. By iterating this process, we are ultimately left with an average of degree 1 polynomials, and geometric progressions.

We require an auxiliary lemma.

Lemma 11.1. Suppose that $\alpha \in \mathbb{K}_\infty$, and $a, g \in A$ satisfy $(a, g) = 1$, g monic, $a \neq 0$, and $|\alpha - a/g| < 1/|g|^2$.

Then one has, for all $\beta \in \mathbb{K}_\infty$,

$$\sum_{|x| \leq q^X} \min \{ q^Y, \|\alpha x + \beta\|^{-1} \} \ll q^{X+Y} (|g|^{-1} + q^{-X} + q^{-Y} + |g|q^{-X-Y}).$$

Proof. We divide up the range of summation into subintervals of the shape

$$I = \{ z + f : \deg(f) < \deg(g) \},$$

with $z \in A$ satisfying $\deg(z) \leq X$. There are $q^{X - \deg(g)}$ possible choices for z . Suppose that x_1, x_2 are distinct elements of a common subinterval I . Then one has

$$\begin{aligned} \|(\alpha x_1 + \beta) - (\alpha x_2 + \beta)\| &= \|\alpha(x_1 - x_2)\| \\ &= \left\| \left(\frac{a}{g} + \gamma \right) (x_1 - x_2) \right\|, \end{aligned}$$

where we write $\gamma = \alpha - a/g$, so that $|\gamma| < 1/|g|^2$. Notice that $|\gamma(x_1 - x_2)| < 1/|g|$ and, since $(a, g) = 1$, one has

$$\left\| \frac{a}{g} (x_1 - x_2) \right\| \geq \left\| \frac{1}{g} \right\| = \frac{1}{|g|}. \text{ Thus}$$

$$\left\| \left(\frac{a}{g} + \gamma \right) (x_1 - x_2) \right\| = \left\| \frac{a}{g} (x_1 - x_2) \right\|.$$

(77)

Hence, we deduce that

$$\begin{aligned} \sum_{x \in I} \min \{ q^Y, \|\alpha x + \beta\|^{-1} \} &\leq q^Y + \sum_{0 \leq \deg(r) < \deg(g)} \left\| \frac{r}{g} \right\|^{-1} \\ &= q^Y + q|g|(1 + 1/q + \dots) \\ &\ll q^Y + |g|. \end{aligned}$$

Adding the contributions from all such intervals I , we conclude that

$$\begin{aligned} \sum_{|x| < q^X} \min \{ q^Y, \|\alpha x + \beta\|^{-1} \} &\ll (q^Y + |g|)(1 + q^X/|g|) \\ &= q^{X+Y} (|g|^{-1} + q^{-X} + q^{-Y} + |g|q^{-X-Y}). \end{aligned}$$

Next, we introduce some standard notation that facilitates the discussion of Weyl differencing. When $\psi: \mathbb{K}_\infty \rightarrow \mathbb{K}_\infty$, we denote by Δ_1 the forward difference operator

$$\Delta_1(\psi(x); h) := \psi(x+h) - \psi(x).$$

We then define Δ_j for $j \geq 2$ recursively by means of the relation

$$\begin{aligned} \Delta_j(\psi(x); \underline{h}) &= \Delta_j(\psi(x); h_1, \dots, h_j) \\ &= \Delta_1(\Delta_{j-1}(\psi(x); h_1, \dots, h_{j-1}); h_j). \end{aligned}$$

By convention, we take $\Delta_0(\psi(x); h) = \psi(x)$.

One may verify that when $1 \leq j \leq k$, one has

$$\Delta_j(x^k; \underline{h}) = h_1 \cdots h_j p_j(x; h_1, \dots, h_j),$$

where p_j is a polynomial in x of degree $\leq k-j$ with (leading) coefficient of x^{k-j} equal to $k! / (k-j)!$. Notice here that

When $\text{char}(\mathbb{F}_q) < k$, then this coefficient may be 0. By the linearity of the operator Δ_j , one sees that

$$\Delta_j (a_k x^k + \dots + a_1 x; \underline{h}) = \sum_{i=1}^k a_i \Delta_j (x^i; \underline{h}),$$

so one may infer the structure of $\Delta_j (p(x); \underline{h})$ easily for general polynomials p . Note that in all cases, when $j > \text{deg}(p)$, one

has $\Delta_j (p(x); \underline{h}) = 0$.

Lemma 11.2. (Weyl differencing) Let $\psi: \mathbb{K}_{\infty} \rightarrow \mathbb{K}_{\infty}$ be any function on \mathbb{K}_{∞} , and put

$$F(\psi) = \sum_{\text{deg}(x) < X} e(\psi(x)).$$

Then for each natural number j , one has

$$|F(\psi)|^{2^j} \ll (q^X)^{2^j - j - 1} \sum_{\text{deg}(h_1) < X} \dots \sum_{\text{deg}(h_j) < X} \sum_{\text{deg}(x) < X} e(\Delta_j(\psi(x); \underline{h})).$$

Proof. We proceed by induction. When $j=1$, one has

$$\begin{aligned} |F(\psi)|^2 &= \sum_{\text{deg}(x) < X} \sum_{\text{deg}(y) < X} e(\psi(y) - \psi(x)) \\ &= \sum_{\text{deg}(x) < X} \sum_{\text{deg}(h_1) < X} e(\psi(x+h_1) - \psi(x)) \\ &= \sum_{\text{deg}(h_1) < X} \sum_{\text{deg}(x) < X} e(\Delta_1(\psi(x); h_1)), \end{aligned}$$

79

Suppose now that the desired conclusion has been established for $1 \leq j < J$. Then by Cauchy's inequality, one has

$$|F(\psi)|^{2^J} = (|F(\psi)|^{2^{J-1}})^2 \\ \ll ((q^x)^{2^{J-1}-J})^2 \left(\underbrace{\sum_{\deg(h_1) < X} \dots \sum_{\deg(h_{J-1}) < X} 1}_{=(q^x)^{J-1}} \right) \Sigma(\psi),$$

where

$$\Sigma(\psi) = \sum_{\deg(h_1) < X} \dots \sum_{\deg(h_{J-1}) < X} \left| \sum_{\deg(x) < X} e(\Delta_{J-1}(\psi(x); \underline{h})) \right|^2_{(h_1, \dots, h_{J-1})}$$

But

$$\left| \sum_{\deg(x) < X} e(\Delta_{J-1}(\psi(x); \underline{h})) \right|^2 = \sum_{\deg(h_J) < X} \sum_{\deg(x) < X} e(\Delta_1(\Delta_{J-1}(\psi(x); \underline{h}); h_J)) \\ = \sum_{\deg(h_J) < X} \sum_{\deg(x) < X} e(\Delta_J(\psi(x); \underline{h}))_{(h_1, \dots, h_J)}.$$

Thus

$$|F(\psi)|^{2^J} \leq (q^x)^{2^{J-1}-2J} \cdot (q^x)^{J-1} \sum_{\deg(h_1) < X} \dots \sum_{\deg(h_J) < X} \sum_{\deg(x) < X} e(\Delta_J(\psi(x); \underline{h})),$$

and the proof follows by induction. //

Note that, if we apply this Weyl differencing lemma ($k-1$ times) to the exponential sum

$$f(x) = \sum_{\deg(x) < X} e(\alpha x^k),$$

then we find that

⑧

$$|f(\alpha)|^{2^{k-1}} \leq (q^X)^{2^{k-1}-k} \sum_{\substack{\deg(h_1) < X \\ \vdots \\ \deg(h_{k-1}) < X}} \sum_{\deg(x) < X} e\left(\overbrace{k! \alpha h_1 \dots h_{k-1} \left(x + \frac{1}{2}(h_1 + \dots + h_{k-1})\right)}^{\Delta_{k-1}(\alpha x^k; h_1, \dots, h_{k-1})}\right)$$

Lemma 11.3. (Weyl's inequality) Let $k \geq 2$ and $\alpha_1, \dots, \alpha_k \in \mathbb{K}_\infty$. Suppose that $a, g \in \mathbb{F}_q[t]$, and $(a, g) = 1$, g is monic and $|\alpha_k - a/g| \leq |g|^{-2}$. Then, provided that $\text{char}(\mathbb{F}_q) > k$, one has

$$\sum_{\deg(x) < X} e(\alpha_k x^k + \dots + \alpha_1 x) \ll (q^X)^{1+\epsilon} \left(|g|^{-1} + q^{-X} + |g|(q^X)^{-k}\right)^{2^{1-k}}$$

Proof. Write $\psi(x) = \alpha_k x^k + \dots + \alpha_1 x$ and

$$F(\underline{\alpha}) = \sum_{\deg(x) < X} e(\psi(x)).$$

We apply the Weyl differencing lemma with $j = k-1$ to obtain the bound

$$|F(\underline{\alpha})|^{2^{k-1}} \ll (q^X)^{2^{k-1}-k} \sum_{\deg(h_1) < X} \dots \sum_{\deg(h_{k-1}) < X} \mathcal{I}(\underline{h}),$$

where

$$\mathcal{I}(\underline{h}) = \sum_{\deg(x) < X} e(\Delta_{k-1}(\psi(x); \underline{h})).$$

Since $\Delta_{k-1}(\psi(x); \underline{h}) = k! h_1 \dots h_{k-1} x \alpha_k + \gamma$, where γ is independent of x , it follows from HW3, QB4 and Lemma 11.1 that

$$\mathcal{I}(\underline{h}) = \begin{cases} q^X, & \text{when } \|k! h_1 \dots h_{k-1} \alpha_k\| < q^{-X}, \\ 0, & \text{when } \|k! h_1 \dots h_{k-1} \alpha_k\| \geq q^{-X}, \end{cases}$$

whence

$$|F(\alpha)|^{2^{k-1}} \ll (q^X)^{2^{k-1}-k} \sum_{\deg(h_1) < X} \dots \sum_{\deg(h_{k-1}) < X} \min \left\{ q^X, \|k! h_1 \dots h_{k-1} \alpha_k\|^{-1} \right\}$$

87

$$\leq (q^X)^{2^{k-1}-k} \left(\sum_{\substack{\deg(g) < (k-1)X \\ 0 \leq \dots}} \tau_k(g) \min \{ q^X, \|g\alpha_k\|^{-1} \} + (q^X)^{k-1} \right)$$

(# h_1, \dots, h_{k-1} s.t. $h_1, \dots, h_{k-1} = 0$)
 $g \neq 0$
 provided that $p = \text{char}(\mathbb{F}_q) > k$.

Theorem 5.2

$$\ll (q^X)^{2^{k-1}-k+\varepsilon} \left(\sum_{0 \leq \deg(g) < (k-1)X} \min \{ q^X, \|g\alpha_k\|^{-1} \} + (q^X)^{k-1} \right)$$

Lemma 11.1

$$\ll (q^X)^{2^{k-1}-k+\varepsilon} q^X \cdot q^{(k-1)X} (|g|^{-1} + q^{-X} + q^{-(k-1)X} + |g|q^{-kX})$$

Hence

$$|F(\alpha)| \ll (q^X)^{1+\varepsilon} (|g|^{-1} + q^{-X} + q^{-(k-1)X} + |g|q^{-kX})^{2^{1-k}}$$

§12. Equidistribution: rational approximations.

We next recall the basic theory of continued fractions as it relates to the function field setting. For any irrational element $\alpha \in K_\infty$, we can write α as an infinite continued fraction in the form

$$\alpha = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \dots}} := [b_0; b_1, b_2, \dots],$$

with $b_i \in \mathbb{F}_q[t]$ and $\deg(b_i) > 0$ ($i \geq 1$). When α is a rational element of K_∞ , on the other hand, one can write α as a finite continued fraction of the shape

$$\alpha = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \dots + \frac{1}{b_n}}}} = [b_0; b_1, \dots, b_n],$$

with $b_i \in \mathbb{F}_q[t]$ and $\deg b_i > 0$ ($1 \leq i \leq n$).

(82)

Note that continued fraction expansions in K_∞ are uniquely defined.

One defines two sequences $(a_n)_{n \geq -2}$ and $(g_n)_{n \geq -2}$ in $\mathbb{F}_q[t]$ recursively by putting

$$a_{-2} = 0, \quad g_{-2} = 1, \quad a_{-1} = 1, \quad g_{-1} = 0,$$

and for $n \geq 0$,

$$a_n = b_n a_{n-1} + a_{n-2} \quad \text{and} \quad g_n = b_n g_{n-1} + g_{n-2}.$$

Then for all $n \geq 0$, we have

$$g_n a_{n-1} - g_{n-1} a_n = (-1)^n \quad \text{and} \quad [b_0; b_1, \dots, b_n] = a_n / g_n.$$

The fractions a_n / g_n ($n \geq 0$) are called the convergents of α .

An inductive argument shows that the sequence $(\deg(g_n))_{n \geq 0}$ is strictly increasing.

We record some simple consequences of these definitions.

Lemma 12.1. Suppose that $\alpha \in K_\infty$. Then the convergents a_n / g_n ($n \geq 0$) of α satisfy the following properties:

(a) one has $\text{ord}(g_n \alpha - a_n) = -\text{ord } g_{n+1}$ ($n \geq 0$);

(b) if $a, g \in \mathbb{F}_q[t]$ satisfy $\text{ord}(g\alpha - a) < -\text{ord } g$, then a/g is a convergent of α ;

Proof: These are easy exercises. //

Lemma 12.2. Let $\alpha \in K_\infty$. Suppose that there exists a constant $x > 1$ such that, for all sufficiently large $N \in \mathbb{N}$, there exist $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t] \setminus \{0\}$ with $\text{ord}(g\alpha - a) \leq -xN$ and

(82)

$\text{ord } g < N$. Then α is rational.

Proof. Suppose that α is irrational and a_n/g_n ($n \geq 0$) are the convergents of α . Since α is irrational, we have $\lim_{n \rightarrow \infty} \deg(g_n) = +\infty$.

We take n sufficiently large and put $N = \text{ord } g_n$.

By hypothesis, we have that there exist $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t] \setminus \{0\}$ such that $\text{ord}(g) < N$ and

$$\text{ord}(g\alpha - a) \leq -kN \leq -\text{ord } g_n = -N < -\text{ord } g. \quad (12.1)$$

Then from Lemma 12.1 (b), we see that a/g is a convergent of α . But $\text{ord } g < N = \text{ord } g_n$, and $(\deg(g_n))_{n \geq 0}$ is strictly increasing, so there exists $m \in \mathbb{N} \cup \{0\}$ with $m < n$ such that $a = a_m$ and $g = g_m$. But then from Lemma 12.1 (a),

$$\text{ord}(g\alpha - a) = \text{ord}(g_m\alpha - a_m) = -\text{ord}(g_{m+1}) \geq -\text{ord } g_n.$$

This contradicts (12.1), and so we are forced to conclude that α is rational. //

We shall apply this conclusion in combination with a consequence of Weyl's inequality. Again we suppose that $\text{char}(\mathbb{F}_q) > k$ and we suppose k to be fixed.

Theorem 12.3. There exist positive constants c and C having the following property. Let $\varepsilon > 0$ and let N be sufficiently large in terms of k, ε . Suppose that $\psi(x) = \alpha_k x^k + \dots + \alpha_1 x$ is a polynomial with coefficients in \mathbb{K}_∞ satisfying the bound

$$\left| \sum_{\deg(x) < N} e(\psi(x)) \right| \geq q^{N-\eta},$$

④ large enough
 for some positive number η with $\eta \leq cN$. Then there exists $a \in \mathbb{F}_q[t]$
 and monic $g \in \mathbb{F}_q[t]$ having the property that

$$\text{ord}(g\alpha_k - a) < -kN + \varepsilon N + C\eta \quad \text{and} \quad \deg(g) \leq \varepsilon N + C\eta.$$

Proof. Suppose that for some positive number η with $\eta \leq cN$ one has

$$\left| \sum_{\deg(x) < N} e(\psi(x)) \right| \geq q^{N-\eta}.$$

Suppose that $a, g \in \mathbb{F}_q[t]$ satisfy $(a, g) = 1$, g monic,
 $\deg(g) \leq kN - 2^{k-1}\varepsilon N - 2^k\eta$ and $|g\alpha_k - a| < q^{-kN + 2^{k-1}\varepsilon N + 2^k\eta} \leq |g|^{-1}$.

Such polynomials exist as a consequence of Dirichlet's approximation
 theorem. By Weyl's inequality (Lemma 11.3), we have

$$\begin{aligned} \left| \sum_{\deg(x) < N} e(\psi(x)) \right| &\ll (q^N)^{1+\varepsilon} \left(|g|^{-1} + q^{-N} + |g|q^{-kN} \right)^{2^{1-k}} \\ &\ll (q^N)^{1+\varepsilon} \left(|g|^{-1} + q^{-N} \right)^{2^{1-k}} + q^{N-2\eta}. \end{aligned}$$

Thus, when N is large, we deduce that

$$\begin{aligned} q^{N-\eta} &\ll (q^N)^{1+\varepsilon} \left(|g|^{-1} + q^{-N} \right)^{2^{1-k}} + q^{N-2\eta} \\ &\Downarrow \\ |g| &\ll \left(q^{N\varepsilon + \eta} \right)^{2^{k-1}} \quad (\text{provided } \eta \leq 2^{-k}N, \text{ say}). \end{aligned}$$

Thus, we have

$$\text{ord}(g\alpha_k - a) < -kN + \varepsilon'N + C\eta \quad \text{and} \quad \deg(g) \leq \varepsilon'N + C\eta,$$

with $\varepsilon' = 2^{k-1}\varepsilon$. The conclusion follows on relabelling ε .

Now we show that when the lower bound in Theorem 12.3 holds too often, then α_k must be rational.

Lemma 12.4. Suppose that $\psi(x) = \alpha_k x^k + \dots + \alpha_1 x$ is a polynomial with coefficients in K_∞ with α_k irrational. Then for any fixed $\eta > 0$, there exists $N_0 \in \mathbb{N}$ having the property that for any $b \in \mathbb{F}_q[t]$, one has

$$\left| \sum_{\deg(x) < N_0} e(\psi(x+b)) \right| < q^{N_0 - \eta}.$$

Proof. Suppose that $\eta > 0$. Suppose further that for any $N \in \mathbb{N}$, if possible, one has the existence of $b_N \in \mathbb{F}_q[t]$ such that

$$\left| \sum_{\deg(x) < N} e(\psi(x+b_N)) \right| \geq q^{N - \eta}. \quad (12.2)$$

Applying Theorem 12.3 with $\varepsilon = 1/3$, we see that there exists a constant $C > 0$ such that, for N sufficiently large, there exists $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ having the property that

$$\text{ord}(g \alpha_k - a) < -kN + \frac{1}{3}N + C\eta \quad \text{and} \quad \deg(g) \leq \frac{N}{3} + C\eta.$$

For each sufficiently large $M \in \mathbb{N}$, we apply these inequalities with $N = \lfloor 3(M - C\eta) \rfloor$. Then

$$\text{ord}(g \alpha_k - a) \leq -(3k-1)M + (3kC\eta + k - \frac{1}{3}) \leq -3M/2$$

and

$$\deg(g) < M.$$

Since these inequalities hold for all large $M \in \mathbb{N}$, we conclude from Lemma 12.2 that α_k is rational. ~~This contradiction~~

86 shows that (12.2) cannot hold, and hence the conclusion of the lemma follows. //

Theorem 12.5. Suppose that $p = \text{char}(\mathbb{F}_q) > k$, and that one at least of $\alpha_1, \dots, \alpha_k \in \mathbb{K}_\infty$ is irrational. Then $(\alpha_k x^k + \dots + \alpha_1 x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in \mathbb{T} .

Proof. We suppose that j is the largest index with α_j irrational.

We then put $\alpha_l = a_l / g_l$, with $a_l, g_l \in \mathbb{F}_q[t]$, g_l monic and $(a_l, g_l) = 1$, for $j < l \leq k$. Finally, put

$$g = \begin{cases} \text{lcm}\{g_{j+1}, \dots, g_k\}, & \text{when } j < k, \\ 1, & \text{when } j = k. \end{cases}$$

We may now largely remove the influence of the rational coefficients from the discussion by breaking down a summation over polynomials $x \in \mathbb{F}_q[t]$ into arithmetic progressions modulo g . We aim to apply Weyl's criterion, so fix $h \in \mathbb{F}_q[t] \setminus \{0\}$. We have, for large X ,

$$\sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < X}} e(h(\alpha_k x^k + \dots + \alpha_1 x)) = \sum_{\substack{r \in \mathbb{F}_q[t] \\ \deg(r) < \deg(g)}} \sum_{\substack{y \in \mathbb{F}_q[t] \\ \deg(y) < X - \deg(g)}} e(h(\alpha_k (yg+r)^k + \dots + \alpha_1 (yg+r)))$$

Since $g \alpha_l \in \mathbb{F}_q[t]$ for $j < l \leq k$ and $h \alpha_k r^k + \dots + \alpha_1 r$ is independent of y , we find that

$$\left| \sum_{y \in \mathbb{F}_q[t]} e(h(\alpha_k (yg+r)^k + \dots + \alpha_r (yg+r))) \right|$$

$$\deg(y) < X - \deg(g)$$

$$= \left| \sum_{y \in \mathbb{F}_q[t]} e(h(\beta_j y^j + \dots + \beta_1 y)) \right|,$$

$$\deg(y) < X - \deg(g)$$

Where $\beta_l = \beta_l(g, r; \underline{\alpha})$ ($1 \leq l \leq r$) and $\beta_j = \alpha_j g^j$. Notice, in particular, that since α_j is irrational, then so too is $h\beta_j$.

Thus

$$q^{-X} \left| \sum_{x \in \mathbb{F}_q[t]} e(h(\alpha_k x^k + \dots + \alpha_r x)) \right| \leq \sum_{r \in \mathbb{F}_q[t]} q^{\deg(g) - X} \left| \sum_{y \in \mathbb{F}_q[t]} e(h(\beta_j y^j + \dots + \beta_1 y)) \right|.$$

$$\deg(x) < X \quad \deg(r) < \deg(g) \quad \deg(y) < X - \deg(g)$$

By Weyl's criterion, the sequence $(\alpha_k x^k + \dots + \alpha_r x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in \mathbb{T} if and only if, for each h , the left hand side converges to 0 as $X \rightarrow \infty$. This is ensured if, for each of the (finitely many) choices for r , one has that for each h ,

$$\lim_{Y \rightarrow \infty} q^{-Y} \left| \sum_{y \in \mathbb{F}_q[t]} e(h(\beta_j y^j + \dots + \beta_1 y)) \right| = 0. \quad (12.2)$$

$$\deg(y) < Y$$

Then we seek a contradiction. Suppose, if possible, that this assertion fails. Given any $\eta > 0$, it follows that there are infinitely many (large) natural numbers N for which

$$\left| \sum_{\substack{y \in \mathbb{F}_q[t] \\ \deg(y) < N}} e(h(\beta_j y^j + \dots + \beta_1 y)) \right| \geq q^{N-\eta}.$$

But Lemma 12.4 shows that there exists $N_0 \in \mathbb{N}$ having the property that for any $b \in \mathbb{F}_q[t]$, one has

$$\left| \sum_{\deg(y) < N_0} e(h(\beta_j y^j + \dots + \beta_1 y)) \right| < q^{N_0 - \eta}.$$

Hence, whenever $N > N_0$, one has

$$\left| \sum_{\deg(y) < N} e(h(\beta_j y^j + \dots + \beta_1 y)) \right| \leq q^{N - N_0} \max_{b \in \mathbb{F}_q[t]} \left| \sum_{\deg(z) < N_0} e(h(\beta_j (z+b)^j + \dots + \beta_1 (z+b))) \right|$$

by writing $y = z + t^{N_0} w$, some $w \in \mathbb{F}_q[t]$ with $\deg(w) \leq N - N_0$.

$$\ll q^{N - N_0} \cdot q^{N_0 - \eta} = q^{N - \eta}.$$

This yields a contradiction. Thus we conclude that (12.2) does in fact hold, and hence

$$\lim_{X \rightarrow \infty} q^{-X} \left| \sum_{\substack{x \in \mathbb{F}_q[t] \\ \deg(x) < X}} e(h(\alpha_u x^u + \dots + \alpha_1 x)) \right| = 0.$$

Then $(\alpha_u x^u + \dots + \alpha_1 x)_{x \in \mathbb{F}_q[t]}$ is equidistributed in \mathbb{T} by

Weyl's criterion. //

§13. An introduction to the circle method in function fields: Waring's problem.

The diophantine version of Waring's problem, posed by Edward Waring in 1770, seeks to determine the least positive integer $s = s(k)$ having the property that all large enough integers n have a representation

$$n = x_1^k + \dots + x_s^k,$$

with $x_i \in \mathbb{N} \cup \{0\}$. Thus, as was famously shown by Lagrange in 1770, all positive integers are the sum of at most 4 integral squares. By convention, the least such integer s is denoted by $G(k)$, and so one has $G(2) = 4$ (the implicit lower bound here is seen by considering integers of the shape $8m+7$, for example).

One has $G(4) = 16$, but aside from the cases $k=2, 4$, no other values of $G(k)$ have been determined. The sharpest known upper bounds are:

$$G(3) \leq 7 \quad (\text{Linnik, 1942}).$$

$$G(5) \leq 17 \quad (\text{Vaughan \& W., 1995})$$

$$G(6) \leq 24 \quad (\text{Vaughan \& W., 1994})$$

⋮

$$G(k) \leq \lceil k (\log k + 4.20032) \rceil \quad (\text{Briden \& W., 2023}).$$

It is conjectured that $G(k) \leq 4k$ in all cases, and that $G(k) \leq k+1$ unless there is a congruential obstruction.

We consider the analogue in function fields — but first we must decide what this analogue should be!

Let k be an integer with $k \geq 2$, let $s \in \mathbb{N}$, and consider a polynomial m in $\mathbb{F}_q[t]$.

Goal: Determine when m has a representation.

90

$$m = x_1^k + \dots + x_s^k,$$

with $x_i \in \mathbb{F}_q[t]$ ($1 \leq i \leq s$)

Observations: (a) It is possible that a representation of a given m fails to exist for all $s \geq 1$. Thus, for example, if $p \mid k$, then

$$x_1^k + \dots + x_s^k \in \mathbb{F}_q[t^p]$$

$$(\text{Note: } (x_0 + x_1 t + \dots + x_\ell t^\ell)^p = x_0^p + x_1^p t^p + \dots + x_\ell^p t^{p\ell}).$$

Then m can be represented as a sum of k -th powers only when $m \in \mathbb{F}_q[t^p]$.

(b) If we are aiming for an analogue of Waring's problem, then we should perhaps insist that each x_i belongs to $\mathbb{F}_q[t]^+$.

This has its problems. Suppose, for example, that $\text{char}(\mathbb{F}_q) = p$ and $\deg(m) = k\ell + 1$. Then at least one of the x_i must have degree $\geq \ell + 1$. But then enough cancellation amongst the degree $k(\ell + 1)$ terms in

$$x_1^k + \dots + x_s^k$$

can occur only when $s \geq p$. Since p might be very large compared to k , this seems like an unnecessarily restrictive condition.

If one does not restrict the x_i at all, on the other hand, then the x_i might have degree arbitrarily large in terms of $\deg(m)$.

This is the approach of Paley (1933), who aims to show that there are polynomials x_1, \dots, x_s with

$$x_1^k + \dots + x_s^k = t.$$

One then finds that

$$x_1 (m(t))^{k\ell} + \dots + x_s (m(t))^{k\ell} = m(t).$$

(91) (c) It could be that the set of all sums of k th powers of elements of $\mathbb{F}_q[t]$ is a proper subring of $\mathbb{F}_q[t]$. Take $k = q^2 - 1$ and π a quadratic irreducible monic polynomial in $\mathbb{F}_q[t]$. Then, when $(x, \pi) = 1$, one has

$$x^k = x^{\varphi(\pi)} \equiv 1 \pmod{\pi}.$$

Then it follows that, whenever $s \in \mathbb{N}$, one has

$$x_1^k + \dots + x_s^k \equiv s' \pmod{\pi},$$

with $0 \leq s' \leq s$, and hence

$$x_1^k + \dots + x_s^k \equiv t \pmod{\pi}$$

is insoluble. We therefore deduce that no polynomial of the shape $\lambda\pi + t$ is represented as the sum of k -th powers in $\mathbb{F}_q[t]$, for any $\lambda \in \mathbb{F}_q[t]$.

For these reasons, it is customary to consider the additive closure of k -th powers in $\mathbb{F}_q[t]$, a ring denoted by

$$\mathbb{J}_q^k[t] := \{x_1^k + \dots + x_s^k : x_i \in \mathbb{F}_q[t] \text{ and } s \in \mathbb{N} \cup \{0\}\}.$$

We say that m is an exceptional element of $\mathbb{J}_q^k[t]$ when its leading coefficient lies in $\mathbb{F}_q \setminus \mathbb{J}_q^k$, and in addition $k \mid \deg(m)$.

The strongest constraint on the degrees of the variables x_i that might still permit a representation $m = x_1^k + \dots + x_s^k$ is

$$\deg(x_i) \leq \lceil (\deg m) / k \rceil \quad (1 \leq i \leq s).$$

We define $P = P_k(m) := \lceil (\deg m) / k \rceil$ when m is not exceptional, and when m is exceptional we put

$$P = P_k(m) := \deg(m) / k + 1.$$

This prevents the obstruction that the lead coefficient of m is not an element of \mathbb{J}_q^k in circumstances wherein $\mathbb{J}_q^k \neq \mathbb{F}_q$.

(92) and $k \mid \deg(m)$.

Notice that when m is not exceptional, then P is the unique integer with $k(P-1) < \deg(m) \leq kP$.

Definition 13.1(a) We say that m admits a strict representation as a sum of s k -th powers when, for some $x_i \in \mathbb{F}_q[t]$ with $\deg(x_i) \leq P_k(m)$ ($1 \leq i \leq s$), one has $x_1^k + \dots + x_s^k = m$ with $q \geq 2$.

(b) When k, q are natural numbers exceeding 1, we define $G_q(k)$ to be the least integer s_0 satisfying the property that, whenever $s \geq s_0$ and $m \in \mathbb{F}_q^k[t]$ has sufficiently large degree (in terms of k, s and q), then m admits a strict representation of the shape $m = x_1^k + \dots + x_s^k$.

Our goal will be a quantitative version of the following theorem.

Theorem 13.2. Suppose that $\text{char}(\mathbb{F}_q) > k$. Then one has $G_q(k) \leq 2^k + 1$.

This is a theorem first proved, more or less simultaneously, by K.R. Matthews (1967), M. Car (1972), R.M. Kubota (1971),

Yu-Ru Liu & W. (2010): $G_q(k) \leq Ak(\log k + \log \log k + 2 + O(\log \log k / \log k))$, whenever $p \nmid k$, where $A = \begin{cases} 1, & \text{when } \text{ch}(\mathbb{F}_q) > k, \\ (1 - 2^{-\gamma_2(k)})^{-1}, & \text{when } \text{ch}(\mathbb{F}_q) < k. \end{cases}$

Hoe,

$\gamma_q(k) = a_0 + a_1 + \dots + a_n$ when $k = a_0 + a_1 p + \dots + a_n p^n$ in base p .