11-09-2013

Now suppose $K/\mathbb{F}_q$, $q = p^e$

Def: An $\mathbb{F}_q$-linear polynomial $f \in K[x]$ is an additive polynomial which also satisfies $f(\alpha x) = \alpha f(x)$, $\alpha \in \mathbb{F}_q$

Theorem: $f \in K[x]$ is $\mathbb{F}_q$-linear iff $f \in K[\tau_q]$, where $\tau_q(x) = x^q$

Proof:

$f \in K[\tau_p]$, let $f = f_0 x + f_1 x^{p} + \cdots + f_n x^{p^n}$

For every $\alpha \in \mathbb{F}_q$ $f(\alpha x) - \alpha f(x) = \sum f_i (\alpha^{p^i} - \alpha) \cdot x^{p^i}$

$= 0 \quad \forall \alpha \in \mathbb{F}_q$

$\Leftrightarrow$ $\alpha^{p^i} = \alpha$ for all α and i s.t. $f_i \neq 0$

$\Leftrightarrow$ $e \mid i$ by Galois theory.

$\Leftrightarrow$ $f_i = 0$ for every $e \nmid i$.

$\Leftrightarrow$ $f \in K[\tau_q]$. ∎

From now on $\tau := \tau_q$, $\mathbb{F}_q$ fixed.

$K[\tau]$ = "polynomial ring in τ" with commutation relation:

$$\tau a = a^q \tau \quad \forall a \in K$$

in particular, $K[\tau]$ is non-commutative unless $K = \mathbb{F}_q$.

Notice: $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_a(\mathbb{C}_\infty)) = \mathbb{C}_\infty[\tau]$.

Def: The formal derivation of $f = f_0 X + f_1 X^2 + \dots + f_n X^{2^n} \in K[\tau]$
$= f_0 + f_1 \tau + \dots + f_n \tau^n$
is

$$df := f_0$$

$$d : K[\tau] \longrightarrow K \qquad \mathbb{F}_q\text{-algebra homomorphism.}$$

3.2) Moore Determinant:

R $\mathbb{F}_q$-algebra, $x_1, \dots, x_n \in R$

Vandermonde determinant:

$$V(x_1, x_2, \dots, x_n) := \det \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & & \\ \vdots & \vdots & & & \\ 1 & x_n & x_n^2 & & x_n^{n-1} \end{bmatrix} = \prod_{1 \le i < j \le n} (x_i - x_j)$$

Similarly, we define the Moore Determinant:

$$M(x_1, \dots, x_n) = \det \begin{bmatrix} x_1 & x_1^2 & \cdots & x_1^{2^{n-1}} \\ x_2 & x_2^2 & & \vdots \\ \vdots & & & \\ x_n & x_n^2 & \cdots & x_n^{2^{n-1}} \end{bmatrix}$$

$$= \prod_{\substack{1 \le i \le n \\ \alpha_1, \dots, \alpha_{i-1} \in \mathbb{F}_q}} \left(x_i + \alpha_{i-1} x_{i-1} + \cdots + \alpha_1 x_1 \right)$$

These factors correspond to representatives of $\mathbb{F}_q^n / \mathbb{F}_q^*$

Instead, multiplying all factors corresponding to non-zero points in $\mathbb{F}_q^n$, we get

$$M(x_1,\dots,x_n)^{q-1} = (-1)^n \prod_{\substack{(\alpha_1,\dots,\alpha_n)\in\mathbb{F}_q^n \\ \neq(0,\dots,0)}} (\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n)$$

Corollary: $M(x_1,\dots,x_n) = 0$ iff $\{x_1,\dots,x_n\}$ are $\mathbb{F}_q$-lin dep.

3.3) Zeros of $\mathbb{F}_q$-linear polynomials

$K/\mathbb{F}_q$ field, K^{alg} algebraic closure, K^{sep} separable closure of K in K^{alg}

$G_K := Gal(K^{sep}/K)$.

Prop: $f \in K[\tau]$ is separable (as an element of $K[x]$) iff $df \neq 0$.

Prop: For any non-zero $f \in K[\tau]$

$$V = \ker f := \{x \in K^{alg} \mid f(x) = 0\}$$

forms an $\mathbb{F}_q$ vector space of $\dim_{\mathbb{F}_q} V \leq \deg_\tau f$.

And $\dim_{\mathbb{F}_q} V = \deg_\tau f$ iff f is separable.

Proof: It is clear that V is an $\mathbb{F}_q$-vector space.

$\#V \leq \deg_x f = q^{\deg_\tau(f)}$ with equality iff f is separable. □

Note: If f is separable, then $V = \ker f$ is a G_K-invariant subspace of K^{sep}. The G_K action on V gives a Galois representation

$$\rho_V : G_K \to \mathrm{Aut}_{\mathbb{F}_q} V \cong GL_n(\mathbb{F}_q).$$

Exercise: If $f = f_0 x + f_1 x^q + \dots + f_{n-1} x^{q^{n-1}} + x^{q^n} \in K[x]$ with $f_0, \dots, f_{n-1}$ alg. indep over $\mathbb{F}_q$ then ρ_V is surjective.

Lends credence to the idea that $S_n = GL_n(\mathbb{F}_1)$.

Theorem: For any G_K-invariant finite dimensional subspace $V \subset K^{sep}$ $\exists!$ monic separable $f_V(x) \in K[x]$ with $\ker f_V = V$.

Proof:

Clearly, $f_V(x) = \prod_{v \in V} (x - v) \in K[x]$ and is sep and monic.

to show that it is $\mathbb{F}_q$-linear:

Let $v_1, \dots, v_n$ be an $\mathbb{F}_q$-basis for V, then

$$f_V(x) = \frac{M(v_1, \dots, v_n, x)}{M(v_1, \dots, v_n)},$$ which is $\mathbb{F}_q$-linear.

(her RHS $\supseteq V$, $\deg_x$ LHS $= \deg_x$ RHS, both sides are monic).

□

Variant: $e_V(x) = x \prod_{v \in V - \{0\}} \left(1 - \frac{x}{v}\right)$ has $\ker e_V = V$

and $d e_V = 1$

One can easily calculate that

$$e_v(x) = \frac{M(v_1, \dots, v_n, x)}{M(v_1, \dots, v_n)^2}.$$

---

6) Lattices in $\mathbb{C}_\infty$:

6.1) Analysis in $\mathbb{C}_\infty$:

Def: An **entire function** $f: \mathbb{C}_\infty \to \mathbb{C}_\infty$ is a power series

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

which converges on all of $\mathbb{C}_\infty$.

(In $\mathbb{C}_\infty$ $\sum_{i=0}^{\infty} b_i$ converges $\iff \lim_{i\to\infty} b_i = 0$)

f is entire $\iff \lim_{n\to\infty} \sqrt[n]{|a_n|} = 0$ (radius of convergence is ∞)

Facts: 1) The set of zeros of an entire function is **strongly discrete**, i.e. any ball of finite radius contains only finitely many of these zeros.

2) An entire function with no zeros is constant.
$\Rightarrow$ every non-constant entire function is surjective.

3) **Weierstrass Product Theorem:**

Let $f: \mathbb{C}_\infty \to \mathbb{C}_\infty$ be an entire function with sequence

(finite or infinite) of non-zero roots $\lambda_1, \lambda_2, \dots$ (with multiplicities). Then

i) $\lim_{i\to\infty} |\lambda_i| = \infty$ (if there are infinitely many zeros)

ii) $f(z) = c \cdot z^n \prod_i \left(1 - \frac{z}{\lambda_i}\right)$ $\quad c \in \mathbb{C}_\infty$, $n = \operatorname{ord}_{z=0}(f)$

Conversely, for any sequence $\lambda_1, \lambda_2, \dots$ satisfying (i), (ii) defines an entire function with zeros $\underbrace{0, 0, \dots, 0}_{n \text{ times}}, \lambda_1, \lambda_2, \dots$.

(3) Follows easily from (a) and (2).

(4.2) A-lattices in $\mathbb{C}_\infty$:

Remark: $A := \bigcap_{p \neq \infty} \mathcal{O}_p$ is defined this way because

it is discrete in F_∞.

Def: An **A-lattice of rank r in $\mathbb{C}_\infty$** is an A-submodule

$\Lambda \subset \mathbb{C}_\infty$ satisfying

i) Λ is strongly discrete

ii) $\Lambda F_\infty \cong F_\infty^r$

(note: for finitely generated A-modules, strongly discrete $\Leftrightarrow$ discrete, but this is not true for infinitely generated A-modules)

(i) + (ii) $\Rightarrow \Lambda$ is a projective A-module of rank r

Def: The exponential function associated to the lattice $\Lambda \subset \mathbb{C}_\infty$ is

$$e_\Lambda(z) := z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right)$$

Prop: $e_\Lambda : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is

1) entire
2) surjective
3) has a simple zero at each $\lambda \in \Lambda$ and no other zeros
4) $\mathbb{F}_q$-linear
5) Λ-periodic (i.e. $e_\Lambda(x+\lambda) = e_\Lambda(x) \quad \forall \lambda \in \Lambda$)

Proof:

(1), (2), (3) clear.

To show (4), write $\Lambda_n := \Lambda \cap B_n(0)$, (ball of radius n in $\mathbb{C}_\infty$) this is a finite $\mathbb{F}_q$-subspace of $\mathbb{C}_\infty$ and so

$$e_{\Lambda_n}(x) = x \prod_{0 \neq \lambda \in \Lambda_n} \left(1 - \frac{x}{\lambda}\right) \in \mathbb{C}_\infty[\tau]$$

and $e_\Lambda(x) = \lim_{n \to \infty} e_{\Lambda_n}(x) \in \mathbb{C}_\infty[[\tau]]$

Now (5) follows from (3) + (4). ∎

So we now have an exact sequence of $\mathbb{F}_q$-modules

$$0 \to \Lambda \to \mathbb{C}_\infty \xrightarrow{e_\Lambda} \mathbb{C}_\infty \to 0$$

Theorem: Let $\Lambda' \subset \Lambda$ be an A-sublattice of the same rank r. Then

i) $e_{\Lambda'}(\Lambda) \cong \Lambda/\Lambda'$ as $\mathbb{F}_q$-spaces

ii) $e_\Lambda(z) = e_{e_{\Lambda'}(\Lambda)}(e_{\Lambda'}(z)) \quad \forall z \in \mathbb{C}_\infty$

where $e_{e_{\Lambda'}(\Lambda)}(x) \in \mathbb{C}_\infty[\tau]$ has $\deg_\tau = \dim_{\mathbb{F}_q}(\Lambda/\Lambda')$.

iii) For each $a \in A$, $\exists\, \varphi_a \in \mathbb{C}_\infty[\tau]$ of $\deg_\tau = r \cdot \deg(a)$
$(\deg(a) = \dim_{\mathbb{F}_q}(A/aA))$

with $d\varphi_a = a$

and $e_\Lambda(az) = \varphi_a / e_\Lambda(z) \quad \forall z \in \mathbb{C}_\infty$.

Proof: Since $\Lambda' \subset \Lambda$ are projective modules of the same rank over the Dedekind domain A, Λ/Λ' is finite.

(i) If $\lambda_1, \lambda_2 \in \Lambda$
then $e_{\Lambda'}(\lambda_1) = e_{\Lambda'}(\lambda_2) \iff e_{\Lambda'}(\lambda_1 - \lambda_2) = 0$
$\iff \lambda_1 \equiv \lambda_2 \ \Lambda'$

so (i) follows.

(ii) $e_{e_{\Lambda'}(\Lambda)}(e_{\Lambda'}(z)) = 0 \iff e_{\Lambda'}(z) = e_{\Lambda'}(\Lambda)$
$\iff z \in \Lambda$

So both sides have the same roots, namely Λ.

$de_{e_{\Lambda'}(\Lambda)}(e_{\Lambda'}(z)) = 1 = de_\Lambda(z)$

so there are no repeated roots, $\dfrac{e_{e_{\Lambda'}(\Lambda)}(e_{\Lambda'}(z))}{e_\Lambda(z)}$ is

entire with no zeros, hence constant, and the constant is 1.

(iii) $a^{-1} e_\Lambda(az) = a^{-1}(az) \prod_{0 \neq \lambda \in \Lambda} \left(1 - \dfrac{az}{\lambda}\right)$

$= z \prod_{0 \neq \lambda \in a^{-1}\Lambda} \left(1 - \dfrac{z}{\lambda}\right) = e_{a^{-1}\Lambda}(z)$

$$= e_{e_\Lambda(a^{-1}\Lambda)}(e_\Lambda(z)) \qquad \text{by (ii)}$$

so (iii) holds with

$$\varphi_a(x) = a\, e_{e_\Lambda(a^{-1}\Lambda)}(x)$$

$$= a x \prod_{h \in e_\Lambda(a^{-1}\Lambda)} \left(1 - \frac{x}{h}\right) \in \mathbb{F}_q[\tau]$$

$$\ker \varphi_a = e_\Lambda(a^{-1}\Lambda) \cong a^{-1}\Lambda/\Lambda \cong \Lambda/a\Lambda \cong (A/aA)^r$$

has dimension $r \cdot \deg a$ over $\mathbb{F}_q$.

$$\Rightarrow \deg_\tau \varphi_a = r \cdot \deg a. \qquad \square$$

Thus we have the diagram

$$\begin{array}{ccccccccc} 0 & \to & \Lambda & \to & \mathbb{C}_\infty & \xrightarrow{e_\Lambda} & \mathbb{C}_\infty & \to & 0 \\ & & \downarrow a & & \downarrow a & & \downarrow \varphi_a & & \\ 0 & \to & \Lambda & \to & \mathbb{C}_\infty & \xrightarrow[e_\Lambda]{} & \mathbb{C}_\infty & \to & 0 \end{array}$$

$\forall a$, $\varphi_a \in \mathbb{C}_\infty[\tau]$

$$\varphi : A \to \mathbb{C}_\infty[\tau] = \mathrm{End}_{\mathbb{F}_q}(\mathbb{C}_a(\mathbb{C}_\infty))$$

$$a \mapsto \varphi_a$$ an $\mathbb{F}_q$-algebra homomorphism

Def: A Drinfeld A-module over $\mathbb{C}_\infty$ is an $\mathbb{F}_q$-algebra homomorphism

$$\begin{aligned} \varphi : A &\longrightarrow \mathbb{C}_\infty[\tau] \\ a &\longmapsto \varphi_a \end{aligned}$$

satisfying:

(i) $d\varphi_a = a$ (normalization)

(ii) $\varphi(A) \not\subset \mathbb{C}_\infty$ (non-triviality)

Can show: $\varphi[a] := \ker \varphi_a \cong (A/aA)^r \quad \forall a \in A$

this r is the rank of φ.