25.3.2021

Remembrances of polynomial values: Fourier's Way

[Joint with K. Soundararajan]

1 - Introduction

Davenport (according to M. Fried):

Q. If f, g are in $\mathbb{Q}[X]$, monic, and

$$\textcircled{*} \qquad f(\mathbb{F}_p) = g(\mathbb{F}_p) \quad \text{(for } p \text{ large enough)}$$

what can one say?

Obvious sol.: $g = f(aX+b)$, $a \neq 0$, $b \in \mathbb{Q}$

("f, g are lin. equiv.", p.e.)

Classical example: 16 is an 8^{th} power modulo every p, $(f(x^8), f(16x^8))$ satisfy $\circledast$, but these are not l.e.

Note that these are decomposable: $g \circ h$, where $\deg(h) \geq 2$.

Th. (Fried) If f and g are indecomposable, then $\circledast \iff f, g$ lin. equiv.

Our problem arises from the natural variant:

what about

(*)' p large enough

for all a, $N(f;a) = N(g;a)$

$$N(f;a) = \sum_{\substack{f(x)=a \\ x \in \mathbb{F}_p}} 1$$

(*)' $\Rightarrow$ (*)

$f_*(\mu_p) = g_*(\mu_p)$ $\Rightarrow$ $\mathrm{Supp}(f_*\mu_p) = \mathrm{Supp}(g_*\mu_p)$

uniform measure on $\mathbb{F}_p$

Consider the discrete Fourier transforms:

$$W(f;h) = \frac{1}{\sqrt{p}} \sum_{a} N(f;a)\, e\left(\frac{ah}{p}\right)$$

$W(f;h) \in \mathbb{F}_p$

$e(z) = e^{2i\pi z}$

$$= \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} e\left(\frac{h f(x)}{p}\right)$$

$(*)' \Longrightarrow (*)$

$(*)' \Longleftrightarrow \widehat{(*)}'$ (discrete Fourier analysis)

$|W(f;h)| = |W(g;h)| \Longleftarrow \widehat{(*)}$

$\widehat{(*)}' \rightsquigarrow W(f;h) = W(g;h)$

Q. [K.-Sound] If $\widehat{(*)}$ holds for p large, what can we say?

Obvious solutions:

$$g = (\pm) f(aX+b) + (\beta)$$

w.l.e

$\pm \rightsquigarrow$ complex conjugate

mult. W by $e\left(\frac{\beta h}{p}\right)$

Theorem [K. – Sound]

f, g in $\mathbb{F}_p[X]$

(1) If $\deg(f) = \deg(g) = d \geq 1$, p large w.r.t. d, and "f and g generic" then $|W(f;h)| = |W(g;h)|$ for all $h \in \mathbb{F}_p$ implies f, g w.l.e over $\overline{\mathbb{F}_p}$.

(2) If f, g are in $\mathbb{Q}[X]$, $\deg f = \deg g = d \geq 1$, and are "generic", then $\widehat{(*)}$ for p large implies f, g w.l.e.

Q. Can one have "indecomposable" in this statement instead of "generic" ?

2 - Ideas of the proof [of (1)]

Tools: (1) Deligne's ℓ-adic Fourier transform

(2) Katz's computation of some "monodromy" groups ($\simeq$ big Galois groups)

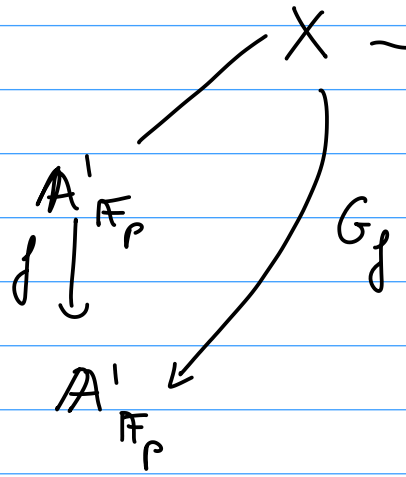
(3) Some group theory (finite groups, compact Lie groups)

Davenport problem

"Sufficiently generic" : some Galois groups are "almost" as big as possible

Ideas of the proof: ($p > d$)

Classical Davenport problem



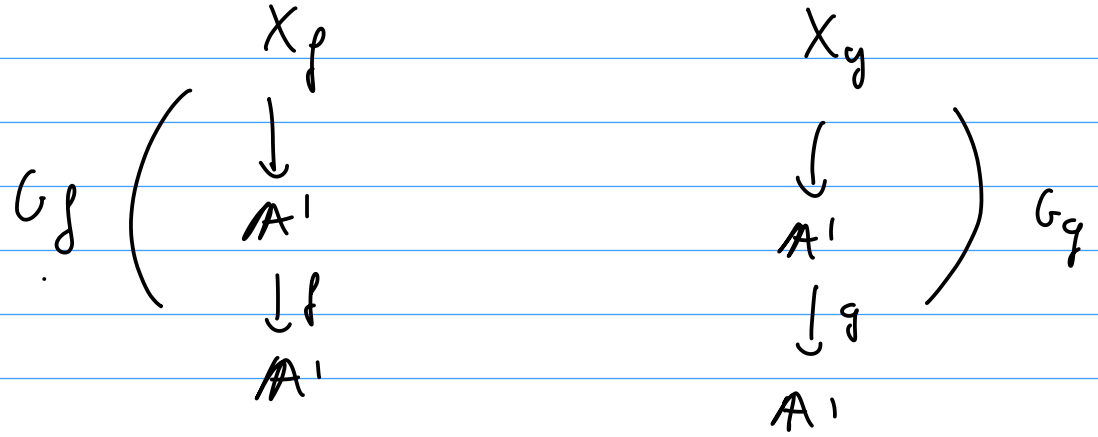
Galois group

[= Gal ($f(Y) = X$, Y indeterminate, base field $\mathbb{F}_p(T)$)]

Fried proved : if f g have the same image (over $\mathbb{F}_{p^r}$ also) and indecomposable ($+ \varepsilon$)

$\deg(f) = \deg(g)$

Then



G_f and G_g are "the same" group G, moreover:

(1) the permutation repr. are isomorphic $\Leftrightarrow$ f, g are l.e.

(2) the associated linear repr. are isomorphic.

clear under $\circledast'$ because characters are given by $N(f;a)$, $N(g;a)$ $(a \in \mathbb{F}_{p^n})$

A construction of Deligne gives "a Fourier side": there exist

$$\pi_1 = \mathrm{Gal}\left(\overline{\mathbb{F}_p(t)}^{sep} / \mathbb{F}_p(t)\right) \xrightarrow{\rho_f} \widehat{G}_f \subset GL_{d-1}(\mathbb{C})$$

$$\downarrow \rho_g$$

$$\widehat{G}_g$$

$$\cap$$

$$GL_{d-1}$$

$$d = \deg(f) = \deg(g)$$

with

$$\mathrm{Tr}\ \rho_f\left(\mathrm{Frob}_h\right) = w(f;h)$$

$$\wr$$

conj. class in π_1

Why is it useful?

$$|W(f;h)| = |W(g;h)| \qquad \forall\, h$$

$$\Updownarrow$$

$$|W(f;h)|^2 = |W(g;h)|^2$$

$$\Updownarrow$$

$$\mathrm{Tr}(\mathrm{Frob}_h \mid \mathrm{End}(\rho_f)) = \mathrm{Tr}(\mathrm{Frob}_h \mid \mathrm{End}(\rho_g))$$

$h \in \mathbb{F}_p$

$\left(V = \mathbb{C}^{d-1} \text{ or } \overline{\mathbb{Q}}_\ell^{\,d-1}\right)$

R.H over finite fields: if $p \geq p_0(d)$ then these equalities for $a \in \mathbb{F}_p$ (essentially) means that $\mathrm{End}(\rho_f) \simeq \mathrm{End}(\rho_g)$.

Q: Given ρ_f, ρ_g, if $\mathrm{End}(\rho_f) \simeq \mathrm{End}(\rho_g)$, what can we say?

We will assume the following "genericity" condition:

(1) The original G_f, G_g are S_d — generic "locally"

(2) The image G_f, G_g are (Zariski-dense) $\subset SL_{d-1}$?

ρ_f, ρ_g are irred.

Theorem (Katz). This holds if

(1) $p > 2d+1$

(2) f has $d-1$ distinct critical values ($f(\beta)$, $f'(\beta)=0$)

$[f \in \bar{\mathbb{F}}_p]$

(3) The critical values S form a Sidon set

($\Leftrightarrow$ $a+b=c+d$ with a,b,c,d in S

$\Rightarrow$ $a=c$ or $a=d$)

Last ingredient

Lemma ("Goursat – Kolchin – Ribet Criterion")

If $\hat{G}_f = \hat{G}_g = SL_{d-1}$ and $\mathrm{End}(\rho_f) \simeq \mathrm{End}(\rho_g)$

then either

(1) $\rho_f \otimes \rho_g$ is irreducible ($\Rightarrow$ not possible under $\circledast$)

(2) $\rho_f \simeq \rho_g$

(3) $\rho_f \simeq \check{\rho}_g$ [contragredient]

w.l.e over $\bar{\mathbb{F}}_p$