TOPICS IN ALGEBRA 4/28

NOTES BY: NATHAN PIERSON

STATEMENT: Let $q = p^r$, $K = \mathbb{F}_q$

$a, b \in \mathbb{F}_q[x]$ polynomials

Take a to be monic, $(a,b) = 1$

Count the number of irreducible monic polynomials inside of $k[x]$ s.t. $f \equiv b \pmod{a}$

$$\varphi(a) = \left| \{ \mathbb{F}_q[x]/(a(x))^\times \} \right|$$

invertible elements

Theorem: The density $\delta\left(f, \begin{smallmatrix}\text{irred. monic} \\ \equiv b \pmod{a}\end{smallmatrix}\right) = \frac{1}{\varphi(a)}$

We'll need to build versions of cyclotomic extensions for function fields (see HW 8)

PROP: Our curve $C = \mathbb{P}^1$

$\{$Irred. monic polynomials $f \in k[x]\}$

$\updownarrow$ bij.

$\{\sum [P] \in \mathrm{Div}(\mathbb{P}^1/k),\ P$ runs in a Galois orbit$\}$

$\rightarrow$ Take f to its roots

$\leftarrow$ In the other direction, go from $\sum [P] \to \prod (x - P)$

So injections exist in both directions

Now we have an easier way to count irred. monic polynomials: the zeta function

Def: Let $\chi : (K[x]/a(x))^* \to \mathbb{C}^\times$

yields $\chi : \mathrm{Div}(\mathbb{P}/K) \to \mathbb{C}$

where $\chi(\sum n_P [P]) = \begin{cases} \prod \chi(\underbrace{\prod (x-P)}_{f \text{ is monic}}{}^{n_P}) \\ 0 \text{ if } f_P \mid a \text{ for some } P \end{cases}$

just as for integers.

Since P varies over a Galois orbit this is well-defined.

Define: $$L(\chi, s) = \sum_{\substack{D \geq 0 \\ D \in \mathrm{Div}(\mathbb{P}^1/k)}} \frac{\chi(D)}{\|D\|^s}$$

$$= \prod_{\substack{\text{Galois orbits} \\ P \mid a(P) \neq 0}} \frac{1}{1 - \frac{\chi(f_P)}{q^{\deg P \cdot s}}}$$

$\|\Sigma [P]\|$

In order to count these irred polynomials we take logs:

$$\log L(\chi, s) = -\sum_{\substack{f \text{ irred.} \\ (f, a) = 1}} \log 1 - \frac{\chi(f)}{q^{\deg f \cdot s}}$$

$$= \sum_{\substack{f \text{ irred.} \\ f \nmid a}} \sum_{n \geq 1} \frac{\chi(f)^n}{n \cdot q^{\deg f \cdot s}} = \sum_{\substack{f \text{ irred.} \\ f \nmid a}} \frac{\chi(f)}{q^{\deg f \cdot s}} + \sum \sum_{n \geq M} \frac{\chi(}{}$$

$O(1)$ s.t.

$$\zeta_C(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$ for any smooth projective C

$$\log \zeta_C\, s = \log P(q^{-s}) - \log(1-q^{-s}) - \log(1-q^{1-s})$$

which behaves like $-\log(s-1) + O(1)$

Define density: $\mathcal{P}$ = a subset of irred. polynomials

$$\delta\mathcal{P} = \lim_{s\to 1^+} \left(\sum_{f\in\mathcal{P}} \frac{1}{q^{\deg f \cdot s}} \right) \Big/ \log(s-1)$$

$$\sum_{\chi \in k[x]/a(x)^*} \chi(\underbrace{fb^{-1}}) = \begin{cases} 0 & f \not\equiv b \pmod a \\ \varphi(a) & \text{if } f \equiv b \pmod a \end{cases}$$

Thus $\varphi(a)\,\delta(\mathcal{P}_{f\equiv 1 \pmod a}) = \varphi(a) \dfrac{\sum_{f\equiv b \pmod a} \frac{1}{q^{\deg p \cdot s}}}{-\log(s-1)}$

$$= \sum_{\chi} \frac{\sum_f \frac{\chi(fb^{-1})}{q^{\deg p \cdot s}}}{-\log(s-1)} = \frac{\sum_\chi \chi(b^{-1}) \sum_f \frac{\chi(f)}{q^{\deg f \cdot s}}}{-\log(s-1)}$$

$$= \sum_\chi \frac{\chi(b^{-1}) \log (L(\chi,s) + O(1))}{-\log(s+1)}$$

$$= \log \zeta_{\mathbb{P}^1}(s) + \sum_{\chi\neq 1} \frac{\chi(b^{-1})(\log L(\chi,s) + O(1)}{-\log(s+1)}$$

$\varphi(a)\,\delta\left(f \equiv b\,(a)\right) = 1 + \lim_{s\to 1} \sum_{\chi\neq 1} \frac{\chi(b^{-1}) \log L(\chi, s)}{\log(s+1)}$

Need to show $L(\chi,1) \neq 0$

Recall for $n \in \mathbb{Z}$, $\chi \in (\mathbb{Z}/n\mathbb{Z})^* \neq 1$

$L(\chi, 1) \neq 0$

Checked zeta function of the nth cyclotomic extension

In the case of this function field

we use that $\zeta(s)$ has a simple pole at $s=1$

$\zeta_{\mathbb{Q}(\zeta_a)}(s)$ has a pole

STATEMENT: FROM HW 8: Take $q = p^r$, $a \in \mathbb{F}_q[x]$ monic

Then there exists $K_a / \mathbb{F}_q$ a Galois extension

such that $\mathrm{Gal}(K_a/\mathbb{F}_q) \cong (\mathbb{F}_q[x]/a(x))^*$

The idea is that you want to define K_a as

$\mathbb{F}_q(\zeta_a)$ where "$\zeta_a^a = 1$" is a "primitive" a^{th} root

Define a special group (p-divisible group)

where this works using Drinfeld modules.

As in the case of number fields, you get that $\exists\, C/\mathbb{F}_q$ smooth projective s.t. the function field $K(C) = K_a$ $\quad C \to \mathbb{P}^1$

$\zeta_C = \zeta_{\mathbb{P}^1} \cdot \prod_{\chi\neq 1} L(\chi, s) \quad \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})} = \frac{1}{(1-q^{-s})(1-q^{1-s})} \prod_{\chi\neq 1} L(\chi$

which is nonzero at $s=1$, so $L(\chi,s)$ is nonzero if $P_C(q^{-1}) \neq 0$, which it is by Riemann hypothesis, which is known for curves.