MATH 549 3-3-10

Note Title 3/3/2010

Recall

Quillen's Thm 1969 The topological FGL over $\pi_* MU$ is isomorphic to Lazard's universal example.

Let F be a FGL over a torsion free ring R. Then over $R \otimes \mathbb{Q}$, F is isomorphic to the additive FGL, i.e. there is a power series $g(x) \in R \otimes \mathbb{Q}[[x]]$ such that

$g(F(x,y)) = g(x) + g(y)$. $g(x)$ is the <u>logarithm</u> of F

Example. Let $F(x,y) = x + y + xy$ (1)

$$1 + F(x,y) = (1+x)(1+y)$$

$$\ln(1 + F(x,y)) = \ln(1+x) + \ln(1+y)$$

and $\ln(1+x) = \sum_{n=1}^{\infty} \frac{x^n}{n}(-1)^{n+1} =: g(x) =: \log(x)$

$$g(F(x,y)) = g(x) + g(y).$$

Thm (Mischenko) In the FGL over $\pi_*(MU)$

$\log x = \sum_{n=1}^{\infty} \frac{[\mathbb{C}P^{n-1}]x^n}{n}$ where $[\mathbb{C}P^{n-1}] \in \pi_{2n-2}(MU)$

Given a FGL F, define power series $[n]_F(x)$ for integers n as follows:

$$\begin{cases} [1]_F(x) = x, \quad [0]_F(x) = 0 \\ [n+1]_F(x) = F(x, [n]_F(x)) \\ [m+n]_F(x) = F([m]_F(x), [n]_F(x)) \end{cases}$$

Example In ①

$$[n](x) = (1+x)^n - 1 = \sum_{k \geq 0} \binom{n}{k} x^k$$

<u>Lemma</u> For a prime p, over R/p

$$[p]_F(x) \equiv \begin{cases} a\,x^{p^n} + \text{higher terms} \mod p \\ \quad \text{for } a \neq 0 \\ 0 \mod p \end{cases}$$

in ① $[p](x) \equiv x^p \mod p$

If $F(x,y) = x+y$, then $[n](x) = nx$

so $[p](x) \equiv 0 \mod p$.

Def. The integer n is the <u>height of F at p</u>.

When $[p](x) \equiv 0$, the height is ∞.

Thm Over an algebraically closed field of char. p, two FGLs are isomorphic iff they have the same height.

Example Let $\log x = \sum_{i \geq 0} \frac{x^{p^{in}}}{p^i} = g(x)$

Honda

$$= x + \frac{x^{p^n}}{p} + \frac{x^{p^{2n}}}{p^2} + \cdots$$

This is the log of a FGL F_n over $\mathbb{Z}_{(p)}$ with height n at p.

$$g^{-1}(g(x)+g(y)) \in \mathbb{Z}_{(p)}[[x,y]]$$

Remark If E is an elliptic, we can choose a local co-ord x at the identity element s.t. the group law for E is a FGL near O.
Its height at a reasonable prime is 1 or 2.

Recall the power series $[n]_F(x)$ for $n \in \mathbb{Z}$. It is can be regarded as an endomorphism of F, i.e.

$$[n]\big(F(x,y)\big) = F\big([n](x), [n](y)\big)$$

If F is defined over a $\mathbb{Z}_{(p)}$-algebra or a $\mathbb{Z}_p$-algebra, we can find power series $[n]_F(x)$ for $n \in \mathbb{Z}_{(p)}$ or $n \in \mathbb{Z}_p$ with similar properties.

Thus we get homomorphisms

$$\left.\begin{array}{l}\mathbb{Z} \\ \mathbb{Z}_{(p)} \\ \mathbb{Z}_p\end{array}\right\} \longrightarrow \operatorname{End}(F)$$

$\leftarrow$ endomorphism ring of F

with $[n]_F(x) \equiv nx \mod (x^2)$

Suppose F be defined over an A-algebra where A is the ring of integers in a number field or a finite extension of $\mathbb{Q}_p$. Can we make sense of $[a]_F(x)$ for $a \in A$?

Def If we can, we say F is a formal A-module.

Lemma (Lubin-Tate 1965) Let A be the ring of integers in a finite extension K of $\mathbb{Q}_p$ with maximal ideal (π) and $A/(\pi) = \mathbb{F}_q$. Let $f(x) \in A[x]$ with

i) $f(x) \equiv \pi x \mod (x^2)$

ii) $f(x) \equiv u x^q \mod (\pi)$ for a unit u

e.g. $f(x) = \pi x + x^q$

Then there is formal A-module F over A for which $[\pi](x) = f(x)$.

They use this to construct field extension of K, namely

$$K_n = K[x] \Big/ \left([\pi^n](x) / x \right)$$

$$\mathrm{Gal}[K_n : K] = \left[A / (\pi^n) \right]^{\times}$$

<u>Example</u> $K = \mathbb{Q}_2[\zeta]/(\zeta^4+1)$

$= \mathbb{Q}_2$[eighth roots of unity]

$A = \mathbb{Z}_2[\zeta]/(\zeta^4+1)$

$\pi = \zeta - 1$

and $\pi^4 = 2 \cdot \text{unit}$

Let $g(x) = \sum_{i \geq 0} \frac{x^{2^i}}{\pi^i} = x + \frac{x^2}{\pi} + \frac{x^4}{\pi^2} + \frac{x^8}{\pi^3} + \cdots$

This is the log of a formal A-module F over A. $[\pi](x) \equiv x^2 \mod \pi$

height is 4. $[2](x) \equiv x^{16} \mod \pi$

Recall the Honda height n FGL

$$\log = \sum_{i \geq 0} \frac{x^{p^{in}}}{p^i}$$

Consider this over $\mathbb{F}_{p^n}$. Its automorphism gp. is S_n, the nth Morava stabilizer gp.

There is a ring $W = W(\mathbb{F}_{p^n})$, the Witt ring for $\mathbb{F}_{p^n}$. It is a degree n extension of $\mathbb{Z}_p$ obtained by adjoining (p^n-1)th roots of unity. It is maximal ideal is (p) and its residue field is $\mathbb{F}_{p^n}$. $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p) = C_n$

generated by the Frobenius map $x \mapsto x^p$.
This automorphism lifts to W and is denoted by $x \mapsto x^\sigma$ where $x^\sigma \equiv x^p \mod p$.
Let $E = W\langle\langle S\rangle\rangle / (S^n - p)$

$$Sw = w^\sigma S \quad \text{for } w \in W.$$

Then $D = E \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a division algebra of rank n^2 over $\mathbb{Q}_p$.
Consider the group of units in E. It is iso to the automorphism

gp of $\mathbb{F}_n \otimes \mathbb{F}_{p^n}$.

Interesting property of D:

Any degree n extension of $\mathbb{Q}_p$ is a subfield of D, e.g. K as above embeds for $n=4$, and the group has an element of order 8.