Lecture 3

- Additive / $\mathbb{F}_q$-linear polynomials
- The Carlitz module

Definition

K be a fld, $P(x) \in K[x]$

P is additive / K if

$$P(\alpha+\beta) = P(\alpha) + P(\beta) \quad \forall \alpha, \beta \in K$$

<u>Very</u> K-dependent

e.g. $P(x) = x^6 + x^4 + x^2 + x \quad / \mathbb{F}_3$

Def: P is absolutely additive if

$$P(\alpha+\beta) = P(\alpha) + P(\beta) \quad \forall \alpha, \beta \in \bar{K}$$

Definition

Let K be a fld of char p and $\tau_p = X^p$

then define

$K\{\tau_p\}$ to be the space spanned by

$$\tau_p^0 = X,\ \tau_p = X^p,\ \tau_p^2 = X^{p^2}, \ldots\ X^{p^i}, \ldots$$

$$\subseteq K[X]$$

Exercise: $K\{\tau_p\}$ is a noncommutative Ring

with $+$ from $K[x]$

$\times$ is composition

$\tau_p^i = x^{p^i}$

Def: $\tau = x^q$, similarly form $K\{\tau\}$

twisted polynomial Ring

Proposition

Let K be infinite of char p. Then P is additive $/K$ iff $P \in K\{\tau_p\}$

2 ingredients

- $\overline{K} \to \overline{K}$ is a fld automorphism
  $x \mapsto x^{\frac{1}{p}}$

  proof: $x \mapsto x^p$ is a fld aut.

- If $P(x) = \sum_{n=0}^{N} a_n x^n$, let $P'(x) = \sum_{n=0}^{N} n a_n x^{n-1}$

proof ($\Leftarrow$) easy if $P \in K\{\tau_p\}$ it is additive

since $(x+y)^p = x^p + y^p$

Assume P is additive

Fix $\alpha \in K$, look at $P(x+\alpha) - P(x) - P(\alpha) \equiv 0$

$$P(x+\alpha) = P(x) + P(\alpha)$$

$$P'(\alpha) = \frac{d}{dx}\left(P(x+\alpha)\right)\Big|_{x=0} = \frac{d}{dx}\left(P(x)+P(\alpha)\right)\Big|_{x=0} = P'(0)$$

$$P(x) = cx + \sum_{j=2}^{N} a_j x^{n_j} \qquad n_j \equiv 0 \pmod p$$

$P(x) = P_0(x) + P_1(x)$ $\quad\quad$ $P_0(x) \in K\{T_p\}$

Notice that P_1 is additive because

$$P_1(x) = P(x) - P_0(x)$$

Let p^e be the largest power of p that divides all the exponents of P_1

$$P_2(x) = P_1(x)^{\frac{1}{p^e}}$$

- this is still additive because $\frac{1}{p^e}$ is a fld aut.

- but P_2 has an exponent that is not $0 \pmod p$ so $P_2(x) \equiv 0$ $\square$

From now on, assume K is infinite of char p.

Definition/Proposition

A polynomial is separable if its roots are distinct in $\overline{K}$. This is the case iff P and P' are relatively prime.

Fundamental Theorem

Let $P \in K[x]$ be separable, $\overset{W}{\overset{\shortparallel}{\{w_1, w_2, \dots, w_m\}}} \subseteq \overline{K}$ be its roots. Then P is additive iff W is a group under addition.

proof: ($\Rightarrow$) if P is additive & w_1, w_2 are 2 roots

then $P(w_1+w_2)=P(w_1)+P(w_2)=0+0=0$

($\Leftarrow$) It is enough to show that

$$P_w(x)=\prod_{i=1}^{m}(x-w_i) \quad \text{is additive}$$

Note that if $w\in W$ then $P_w(x+w)=P_w(x)$

Fix $y\in K$, $H(x)=P_w(x+y)-P_w(x)-P_w(y)$

$\deg H < \deg P = m$

But every $w\in W$ is a root of H, so $H\equiv 0$

Let y be an indeterminate

$$H_1(y) = P_w(x+y) - P_w(x) - P_w(y) \in K[x,y]$$

$$K[x][y]$$

$$H_1(\alpha) = 0 \quad \forall \alpha \in K$$

& K is infinite

So $H_1(y) \equiv 0$

So P_w is additive

$\square$

Upgrade everything to $\mathbb{F}_q$-linearity

Def: P is $\mathbb{F}_q$-linear if it is additive and

$$P(\zeta x) = \zeta P(x) \quad \forall \zeta \in \mathbb{F}_q$$

Proposition

P is $\mathbb{F}_q$-linear iff $P \in K\{\tau\}$ $\qquad (\tau = X^q)$

Fundamental Theorem

Let P be separable, W its roots. Then P is $\mathbb{F}_q$-linear iff W is an $\mathbb{F}_q$-vector space

Analogy

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathbb{R}$	$\mathbb{F}_q((\frac{1}{T})) = K_\infty$
$\mathbb{C}$	$C_\infty = \widehat{\overline{K_\infty}}$
e^z	?

Classical interlude

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Notice $\quad e^{nz} = (e^z)^n$

$$e^{(n+m)z} = e^{nz} \cdot e^{mz}$$

$$\mathbb{Z} \curvearrowright \mathbb{C} \qquad \begin{array}{ccc} \mathbb{C} & \xrightarrow{\exp} & \mathbb{C}^\times \\ {\scriptstyle nz}\downarrow & & \downarrow{\scriptstyle z^n} \\ \mathbb{C} & \xrightarrow{\exp} & \mathbb{C}^\times \end{array} \qquad \mathbb{Z} \curvearrowright \mathbb{C}^\times$$

Exp gives $\mathbb{C}^\times$ a new $\mathbb{Z}$-module structure

Torsion points of this "new" action

$$z \in \mathbb{C}^\times : \quad z^n = 1$$

They are the roots of unity!

Theorem

Every abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$

$$e_c(z) = \sum_{n=0}^{\infty} \frac{z^{q^n}}{D_n}$$

$$D_n = \prod_{\substack{a \text{ monic} \\ \text{of deg } n}} a$$

Proposition

Let $z \in C_\infty$

$$e_c(Tz) = Te_c(z) + e_c(z)^q$$