Definition: A scheme T is of finite order r over S, if $T = \mathrm{Spec}\,\mathcal{A}$ is a sheaf of $\mathcal{O}_S$-algebras, which is locally free of rank r

(Locally free of constant finite rk $\overset{\Rightarrow}{\Leftarrow}$ finite + flat)

needs S locally noeth + conn

Suppose $G = \mathrm{Spec}(\mathcal{A})$ is a commutative gp scheme of finite order over S.

Consider the map $m_G : G \longrightarrow G$

s.t. $g \longmapsto g^m$

$g \in G(T)$ for T/S

In the first part, we look at 2 theorems:

- Theorem (Deligne) – A commutative S-group of order m is killed by m i.e. $m_G = 0_G$
  or $g^m = e$

- Theorem 1 – An S-group of order p is commutative

Notation :

(1) $G = \mathrm{Spec}(\mathcal{A})$ is a group scheme of finite order over S.

(2) We have maps :

- $s_{\mathcal{A}} : \mathcal{A} \to \mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{A}$ (comultiplication)

$$\updownarrow$$

$$G \times G \longrightarrow G \quad \text{(law of composition)}$$

- $t_{\mathcal{A}} : \mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{A} \longrightarrow \mathcal{A}$ (alg multiplication)

$$\updownarrow$$

$$G \xrightarrow{\Delta} G \times G$$

(3) Let $\mathcal{A}'$ denote the $\mathcal{O}_S$-linear dual of $\mathcal{A}$

$$\mathcal{A}' := \mathcal{H}om_{\mathcal{O}_S}(\mathcal{A}, \mathcal{O}_S)$$

As $\mathcal{A}'$ is locally free of same rank as $\mathcal{A}$,

$$(\mathcal{A}' \otimes \mathcal{A}') \cong (\mathcal{A} \otimes \mathcal{A})'$$

& we have

$$t_{\mathcal{A}'} = (s_{\mathcal{A}})' : \mathcal{A}' \otimes_{\mathcal{O}_S} \mathcal{A}' \longrightarrow \mathcal{A}'$$

(ass. because $s_{\mathcal{A}}$ is associative

{ Commutative iff $s_{\mathcal{A}}$ is commutative iff G is commutative)

only barrier to taking relative spec of $\mathcal{A}'$

$$s_{\mathcal{A}'} = (t_{\mathcal{A}})' : \mathcal{A}' \longrightarrow \mathcal{A}' \otimes \mathcal{A}'$$

(commutative & associative as $t_{\mathcal{A}}$ is)

If G is commutative, $\mathrm{spec}(\mathcal{A}')$ is a commutative gp scheme, with unit & counit dualizing counit & unit resp of $\mathcal{A}$ (Cartier dual)

Note :

$$G(S) = \mathrm{Hom}_{\mathcal{O}_S\text{-alg}}(A, \mathcal{O}_S) \hookrightarrow \Gamma(S, A')$$

Claim : This gives an isomorphism of $G(S)$ into the multiplicative group of invertible elements $g \in \Gamma(S, A')$ such that $s_{A'}(g) = g \otimes g$

(These are the characters of G'. $\therefore$ G = character gp scheme of G')

Pf :

Note : • $s_{A'}(f) = f \otimes f$

$\Leftrightarrow$ $(f \circ t_A)(a \otimes b) = (f \otimes f)(a \otimes b)$

$\Leftrightarrow$ $f(ab) = f(a)f(b)$

• f invertible $\Leftrightarrow$ $\exists g :$ $t_{A'}(f \otimes g) = \varepsilon$ counit in A

$$\overset{\parallel}{(f \otimes g) \circ s_A}$$

Now, If $f \in G(S)$,

$s_{A'}(f) = f \otimes f$ & $\exists f^{-1} \in G(S)$ & $t_{A'}(f \otimes f^{-1}) = \varepsilon$

$\therefore$ f is invertible

OTOH if f is invertible & satisfies $s_{A'}(f) = f \otimes f$

$(f \otimes g) \circ s_A(1) = \varepsilon(1)$

$\Rightarrow$ $f(1)g(1) = 1$

$\Rightarrow$ $f(1)$ is a unit

$f(1) = f(1 \cdot 1) = f(1)^2$

$\Rightarrow f(1) = 1$

$\therefore$ $f \in G(S)$

So if G is commutative,

$\mathcal{A} \xrightarrow{\sim} (\mathcal{A}')'$

$\therefore G \xrightarrow{\sim} (G')'$

$$\begin{array}{ccccc} G(T) = G_T(T) & \xrightarrow{\sim} & \mathrm{Hom}_{T\text{-gps}}(G'_T, \mathbb{G}_{m,T}) & & \forall T/S \\ g & \longmapsto & (g \longleftarrow t) & & \\ & & {\scriptstyle \in G(T) \subset A'_T} & & \end{array}$$

$$\begin{array}{ccc} G(T) & \longrightarrow & \mathrm{Hom}_{gp}(G'(T), \mathbb{G}_{m,S}(T)) \\ & & \updownarrow \\ G \times_S G' & \longrightarrow & \mathbb{G}_{m,S} \end{array}$$

(Cartier pairing)

E.g. If Γ is a finite gp. $\underline{\Gamma}_{\mathrm{Spec}\, R}$, constant gp scheme has Cartier dual given by $\mathrm{Spec}\, R[\Gamma]$

Theorem: A commutative S gp $G = \mathrm{Spec}(\mathcal{A})$ of order m is killed by m_G

Idea of pf: let Γ be abstract gp of order m & let $x \in \Gamma$

$$\prod_{\gamma \in \Gamma} \gamma = \prod (\gamma x) = \left(\prod \gamma\right) x^m$$

$$\Rightarrow x^m = 1$$

To apply the idea, Deligne defines a trace map:

Suppose $T = \mathcal{S}pec(\mathcal{B})$ is a scheme of order m over S

$(\mathcal{A} \otimes \mathcal{O}_T)'$ as a sheaf on T

pushforward of $\mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{A}'$ $\because T \to S$ is affine

$$\begin{tikzcd}
G(T) \arrow[r, hook] \arrow[d, dashed, "\mathrm{Tr}"] & \Gamma(T, \underbrace{\mathcal{O}_T \otimes_{\mathcal{O}_S} \mathcal{A}'}_{=(\mathcal{A}\otimes\mathcal{O}_T)'}) = \Gamma(S, \mathcal{B} \otimes_{\mathcal{O}_S} \mathcal{A}') \arrow[d, "N"] \\
G(S) \arrow[r, hook] & \Gamma(S, A')
\end{tikzcd}$$

locally free of rk m over $\mathcal{A}'$

N = norm
an $\mathcal{O}_S$ alg map

Note : 1) Under N, invertible elts go to inv. elts

2) Claim : If $S_{\mathcal{A}' \otimes \mathcal{B}}(f) = f \otimes f$

then $S_{\mathcal{A}'}(N(f)) = N(f) \otimes N(f)$

Pf of claim :

First, note that if $R' \xrightarrow{\varphi} R''$ is an alg hom
B/R, free of finite rk

$$\begin{tikzcd}
B \otimes_{\mathcal{O}_S} R' \arrow[r, "1\otimes\varphi"] \arrow[d, "N"] \arrow[dr, phantom, "\circlearrowright"] & B \otimes_{\mathcal{O}_S} R'' \arrow[d, "N"] \\
R' \arrow[r, "\varphi"] & R''
\end{tikzcd}$$

Let $\{e_i\}$ give a basis of B over ground rg

$f \in B \otimes_R R'$ $\quad f(e_j \otimes 1) = \sum \mu_{ij}(e_i \otimes 1) = \sum e_i \otimes \mu_{ij}$

$(1\otimes\varphi) f \cdot (1 \otimes \varphi)(e_j \otimes 1) = \sum e_i \otimes \varphi\mu_{ij}$

$\therefore \quad N(f) = \det \mu_{ij} \xmapsto{\varphi} \det \varphi\mu_{ij} = N((1\otimes\varphi)f)$

Apply to

$$\begin{tikzcd}
B \otimes_{\theta_S} A' \arrow[rr, "{id \otimes S_{A'} \,=\, S_{B\otimes A'}}"] \arrow[d, "N"] & & B \otimes_{\theta_S} A' \otimes A' \arrow[d, "N"] \\
A' \arrow[rr, "S_{A'}"] & & A' \otimes_{\theta_S} A'
\end{tikzcd}$$

For f in $G(T)$, $S_{A'}(N(f)) = N(S_{B\otimes A'} f) = N(f \otimes_B f)$

Apply to

$$\begin{tikzcd}
B \otimes_{\theta_S} A' \arrow[rr, "id \otimes 1"] \arrow[d] & & B \otimes_{\theta_S} A' \otimes A' \arrow[d] \\
A' \arrow[rr, "id \otimes 1"] & & A' \otimes A'
\end{tikzcd}$$

$f \mapsto f \otimes 1$

$f \mapsto N(f)$

$$N(f) \otimes 1 = N(f \otimes 1)$$

$$\therefore N(f \otimes f) = N(f \otimes 1)\, N(1 \otimes f) = (N(f) \otimes 1)(1 \otimes N(f))$$

$$= N(f) \otimes N(f)$$

$\therefore$ if $f \in G(T)$, $N(f)$, being invertible as well, $\in G(S)$.

Tr is a gp homomorphism

$$Tr_f(u) = u^m \quad \forall\, u \in G(S) \subset G(T)$$

If $t : T \longrightarrow T$ is an S-automorphism.

then $Tr(f) = Tr(T \xrightarrow{t} T \xrightarrow{f} G) \quad \forall f \in G(T)$
because t locally induces a rearrangement of basis of B

Pf of Theorem:

We want to show that if $u \in G(S)$, then $u^m = 1$
(Enough $\because$ we can vary base scheme & see every pt as a map from the base scheme)

Let $t_u : G \longrightarrow G$ be the translation on G by u

$$\left(G \xrightarrow{\sim} G \times_S S \xrightarrow{id,\, u} G \times_S G \longrightarrow G \right)$$

Consider $id \in G(G)$

$$Tr(id) = Tr\left(\begin{array}{ccccc} G & \xrightarrow{t_u} & G & \xrightarrow{id} & G \\ g & \mapsto & gu & \longmapsto & gu \end{array} \right)$$

$$id \circ t_u : \quad \underset{id}{\overset{G(G)}{\in}} \longmapsto id * u$$

$$\therefore id \circ t_u = id * u \quad : G \longrightarrow G$$

$$Tr(id) = Tr(id \circ t_u) = Tr(id * u)$$
gp. in G / alg. in A'

$$= Tr(id)\, Tr(u)$$
$$= Tr(id) * u^m$$

$$\Rightarrow \quad u^m = 1$$

Theorem 1 : An S gp of order p is commutative & killed by p

(Only need to show commutativity)

Pf : Reduce to the case that $S = \operatorname{Spec} R$ affine. $G = \operatorname{Spec} A$

$$0 \longrightarrow \ker \longrightarrow A \xrightarrow{S_A - S_A \circ \text{swap}} A \otimes A$$

STS that at each local rg, ker is 0,

$\therefore$ WMA R is local

Can embed R in a (strictly henselian) local rg R^{sh} w/ residue field $k = k^s$

$$A \hookrightarrow A \otimes_R R^{sh}$$

& STS $G_{R^{sh}}$ is commutative

So WMA R is local w/ residue field $k = k^s$

Lemma : Let $k = k^s$. $G = \operatorname{Spec} A$ be a k-gp of order p. Then either G is the constant gp scheme, or char $k = p$ &

$G = \mu_{p,k}$

$G = \alpha_{p,k}$

In particular, G is commutative & A is gen by a single elt

Pf of thm granting Lemma :

$G_k = \mathrm{Spec}(\underbrace{A \otimes_R k}_{= \bar{A}})$ is comm. by Lemma

$A' \otimes_R k =$

$\therefore (\bar{A})'$ has comm Hopf alg structure

Apply lemma to $(G_k)'$, the Cartier dual of G_k.

Let $x \in A'$ be s.t. $\bar{x} \in A' \otimes_R k = (\bar{A})'$ generates $A' \otimes_R k$

Then $\overline{R[x]} = R[x] \otimes k = k[\bar{x}] = A' \otimes k$

By Nakayama $R[x] = A' \Rightarrow A'$ is commutative

$\Rightarrow G$ is commutative

Now pf of Lemma 1 :

Notice : $G^\circ \subset G$ is a normal subgp scheme

Fact : G/G° is well defined gp scheme of finite order

& $\mathrm{ord}\, G =: \underset{\overset{\parallel}{p}}{|G|} = |G/G^\circ| \cdot |G^\circ|$

$\therefore$ I. G° is order 1 over k $\Leftrightarrow G^\circ = \mathrm{Spec}\, k$

or

II. G° is order p $\Leftrightarrow G^\circ = G$

I. $\Leftrightarrow G$ étale / k

$\Leftrightarrow G = \coprod_{g \in G(k)} \mathrm{Spec}\, k \quad \therefore G \cong \underline{G(k)}_k$

$\underset{\substack{\uparrow \\ \because \text{ order} = p}}{\cong} \underline{\mathbb{Z}/p\mathbb{Z}}_k$

A is gen by any function $(a_i)_{i \in \mathbb{Z}/p\mathbb{Z}}$ which takes distinct values at the pts of $\mathbb{Z}/p\mathbb{Z}$ because any equation that it satisfies over k will have at least p distinct solutions $\therefore$ the equation will have deg $\geq p$.

II. $\Leftarrow$ G is connected :

G/k is finite, $\therefore$ noetherian + dim $A = 0$ (all pts are closed pts & each will give a distinct irr component. More than 1 pt $\Rightarrow$ disconnected)

$\therefore$ exactly 1 closed pt

$\therefore A = (A, \mathfrak{m})$ is a local noeth rg of dim 0.
The augmentation ideal (giving the counit) $\mathfrak{m}$ is nilpotent.
$\left[A \xrightarrow{\varepsilon} k \Rightarrow A = k \oplus \ker \varepsilon \subset$ prime ideal $\therefore \overset{\shortparallel}{\mathfrak{m}}$; $\therefore A/\mathfrak{m} = k \right]$

As order $G = p$, $\mathfrak{m} \neq \mathfrak{m}^2$ (else $\mathfrak{m} = 0$ by Nakayama & order $= 1$)

let $d \overset{\neq 0}{} \in \mathrm{Hom}_A(\Omega_{A/k}, k) = (\mathfrak{m}/\mathfrak{m}^2)^\vee$

$d \in \mathfrak{m}' \subset A'$ $\qquad S_{A'}(d) : \underset{\underset{A \otimes A}{\uparrow}}{a \otimes b} \longmapsto ab \longmapsto d(ab) = \bar{a}\,db + \bar{b}\,da$

$\therefore S_{A'}(d) = \underset{\text{unit of the alg } k[d] \subset A'}{\underset{\uparrow}{\varepsilon}} \otimes d + d \otimes \varepsilon \subset k[d] \otimes k[d]$

$\therefore k[d] \subset A'$

We have $A = A'' \twoheadrightarrow \underset{\underset{k}{\neq}}{k[d]'} \Rightarrow$ order of $k[d]' = p$

$\Rightarrow \underset{\uparrow \text{commutative}}{k[d]} = A'$

$\therefore$ we can take $G' = \operatorname{Spec} A'$

G' is étale or connected

G' étale $\Rightarrow$ $G' = \underline{\mathbb{Z}/p\mathbb{Z}}_k$

$\Rightarrow G = (G')' = \mu_{p,k} = \operatorname{Spec}\left(\dfrac{k[X]}{X^p - 1}\right)$

As G is connected, char $k = p$.

G' connected $\Rightarrow$ d nilpotent & $k[d]$ is of rk p.

$\therefore d^{p-1} \neq 0$ & $d^p = 0$

(By Artin Rees, Basically $(d^i) \supset (d^{i+1}) \supset \dots$ doesn't stabilize unless we get to $d^n = 0$, so we will keep losing dimension until n $\therefore n \leq p$. but $k[d]$ is rk p $\therefore$ $n \geq p$)

$S_{A'}$ is a rg hom $\therefore$

$$0 = S_{A'}(d^p) = (S_{A'}(d))^p = (1 \otimes d + d \otimes 1)^p$$

$\Rightarrow p = 0$ $\Rightarrow$ char $k = p$

As $S_{A'}(d) = d \otimes 1 + 1 \otimes d$,

$G' = \alpha_{p,k}$

$G = (G')' = \alpha_{p,k}$ (φ, dual of d ends up going to $\varphi \otimes 1 + 1 \otimes \varphi$ under S_A)

So now we wish to classify these gp schemes

Let $\chi : \mathbb{F}_p \longrightarrow \mathbb{Z}_p$ be the multiplicative section of $\mathbb{Z}_p \longrightarrow \mathbb{F}_p$

So, $\chi(0) = 0$ & for $m \in \mathbb{F}_p^*$, $\chi(m)$ is the unique $(p-1)$ root of unity in $\mathbb{Z}_p$ whose residue is m mod p.

$\chi|_{\mathbb{F}_p^*}$ generates the gp $\mathrm{Hom}_{gp}(\mathbb{F}_p^*, \mathbb{Z}_p^*)$

Let $\Lambda_p := \mathbb{Z}\left[\chi(\mathbb{F}_p), \frac{1}{p(p-1)}\right] \cap \mathbb{Z}_p \subset \mathbb{Q}_p$

So we are attaching the p-1 roots of unity

$$\begin{array}{c} \mathrm{Spec}\ \mathbb{Z}[\chi(\mathbb{F}_p)] \\ \downarrow \pi \\ \mathrm{Spec}\ \mathbb{Z} \end{array} \quad - \quad \{\pi^{-1} D(p-1),$$ all primes lying over p except the one prime that gives the embedding $\mathbb{Z}[\chi(\mathbb{F}_p)] \to \mathbb{Q}_p\}$

$\Lambda_p \cap p\mathbb{Z}_p = p\mathbb{Z}_p$

$\uparrow$ $\because$ unramified over p

Fix p, & let $\Lambda = \Lambda_p$

Set up :

$$\begin{tikzcd} G = \mathrm{Spec}\,\mathcal{A} \arrow[d, dash, "\text{order } p"] \\ S \arrow[d, dash] \\ \mathrm{Spec}\,\Lambda \end{tikzcd}$$

(so we take $\chi(m)$ as taking values in $\Gamma(S, \mathcal{O}_S)$)

By Thm 1 $\quad \mathbb{F}_p^* \curvearrowright G$

$$m \longmapsto \left(\begin{array}{ccc} G & \xrightarrow{\text{gp hom}} & G \\ g & \longmapsto & g^{m \bmod p} \\ e & \longmapsto & e \end{array} \right)$$

$$m \longmapsto \left(\begin{tikzcd} \mathcal{A} \arrow[dr, "\varepsilon"'] & \mathcal{A} \arrow[l, "{[m]}"'] \arrow[d, "\varepsilon"] \\ & \mathcal{O}_S \end{tikzcd} \right)$$

$\mathcal{A} = \mathcal{O}_S \oplus \mathcal{I}$

$\mathcal{A}$ & the augmentation ideal $\mathcal{I}$ are sheaves of modules over the group algebra $\mathcal{O}_S[\mathbb{F}_p^*]$. We will use this action to probe the structure of $\mathcal{I}$

Define $\quad e_i = \dfrac{1}{p-1} \displaystyle\sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m)\,[m] \in \mathcal{O}_S[\mathbb{F}_p^*]$

(depends only on i mod $p-1$)

Check : $\quad e_i e_j = 0$ if $i \neq j$ (the pt is that $\displaystyle\sum_{r \in \mathbb{F}_p^*} \chi^{i-j}(r)$ is a sum of the form $1 + \zeta + \zeta^2 + \dots + \zeta^{p-1}$ for $\zeta \neq 1$ some $p-1$ root of unity)

$e_i^2 = 1$

$$\sum e_i = [1] = id$$

$$[m] e_i = \chi^i(m) e_i$$

Let $\mathcal{I}_i := e_i \mathcal{I}$

$$\Rightarrow \mathcal{I} = \bigoplus_{i=1}^{p-1} \mathcal{I}_i$$

$$\mathcal{I}_i(U) = \{ f \in \mathcal{I}(U) : [m] f = \chi^i(m) f \quad \forall m \in \mathbb{F}_p^\times \}$$

$$\underset{\uparrow}{=} \{ f \in \mathcal{I}(U) : [m] f = \chi^i(m) f \quad \forall m \in \mathbb{F}_p \}$$

$\because [0] f = 0 \quad \because [0] = \varepsilon \quad \& \ f \in \mathcal{I}(U)$

$$\Rightarrow ([m] f)([m] g) = [m](fg) \Rightarrow \mathcal{I}_i \mathcal{I}_j \subset \mathcal{I}_{i+j}$$

Since $\mathcal{I}$ is locally free of rk $p-1$ over $\mathcal{O}_S$, $\mathcal{I}_i$ is locally f.p. projective modules, $\therefore$ locally free of rk r_i &

$$\sum r_i = p-1$$

To compute rank, we can pass to a geometric pt

So assume $S = \operatorname{Spec}(k)$, $k = \bar{k}$. $G = \operatorname{Spec} A$, $\Gamma(G, \mathcal{I}_i) = I_i$

We will find $f \in I_1$ st. $f_1^i \neq 0 \quad \forall i \in [1, p-1]$ $\therefore$

$\operatorname{rk} I_i \geq 1 \quad \forall i \quad \therefore \operatorname{rk} I_i = 1$

By Lemma earlier, we have 3 possibilities for G.

1. $G = \underline{\mathbb{Z}/p\mathbb{Z}}_k$
2. $G = \alpha_{p,k}$ char $k = p$
3. $G = \mu_{p,k}$ char $k = p$

In case 1., $G = \underline{\mathbb{Z}/p\mathbb{Z}}_k$. A is the algebra of k-valued functions on $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ &

Let $f_1 = \chi$ $\quad \chi(0) = 0 \quad \therefore \quad \varepsilon(\chi) = pr_0(\chi) = 0$

$\therefore \chi \in I.$

$([m]\chi)(n) = \chi(mn) = \chi'(m)\chi(n)$

$\therefore \chi \in I_1$

In case 2., 3., $G \cong \alpha_{p,k}$ or $\mu_{p,k}$ & char $k = p$

For $\alpha_{p,k}$ $\quad A = k[t]$ with $t^p = 0$, $S_A t = t \otimes 1 + 1 \otimes t$

$$\therefore [m]t\,(\underset{t \mapsto t}{id})$$

$$= t(\underset{t \mapsto mt}{id^m})$$

$$= mt$$

For $\mu_{p,k}$ $\quad A = \dfrac{k[s]}{s^p - 1} \underset{t = s-1}{=} \dfrac{k[t]}{t^p}$

$$[m]s\,(id)^{s \mapsto s}$$

$$= s(\underset{s \mapsto s^m}{id^m})$$

$$\therefore [m]s = s^m$$

$$\therefore [m]t = s^m - 1 = (t+1)^m - 1$$

$$[m]t \equiv mt \underset{\substack{\chi(m) = m \\ m \text{ char } p}}{=} \chi(m)t \mod t^2$$

$$\approx \sum_i \chi(m)\, e_i t$$

$$[m]t = \sum_i [m]\, e_i t = \sum_i \chi^i(m) e_i t$$

$$\Rightarrow 0 \neq t \equiv e_i t \mod t^2$$

Let $f_1 = e_1 t$

So we get that over alg closed fields,

$$I_1^i = I_i$$

Locally on $\operatorname{Spec} R \subset S$, $\mathcal{I}(\operatorname{Spec} R) = I$, we have

$$\text{for } i \in [1, p-1] \qquad 0 \neq \left(I_1 \otimes_R \kappa(p) \otimes_{\kappa(p)} \overline{\kappa(p)}\right)^i \subset A \otimes_R \overline{\kappa(p)}$$

$$\uparrow$$

$$I_1^i \otimes_R \overline{\kappa(p)}$$

$$\Rightarrow I_1^i \neq 0$$

$$\Rightarrow I_1^i \otimes \kappa(p) = I_i \otimes \kappa(p) \quad \forall p$$

Nakayama $\Rightarrow$ $I_1^i = I_i$

To conclude, we have the following lemma:

- $\mathcal{I} = \bigoplus_{i=1}^{p-1} \mathcal{I}_i$.
- For $i \in [1, p-1]$, $\mathcal{I}_i$ is invertible $\mathcal{O}_S$-module consisting of local sections of A s.t. $[m]f = \chi^i(m) f \quad \forall m \in \mathbb{F}_p$
- $\mathcal{I}_i \mathcal{I}_j \subset \mathcal{I}_{i+j} \quad \forall i, j$
- $\mathcal{I}_1^i = \mathcal{I}_i \quad \forall i \in [1, p-1]$

<u>Example</u> :

$$\mu_{p,\Lambda} = \operatorname{Spec} B \quad \text{where} \quad B = \frac{\Lambda[z]}{z^p - 1}$$

$$S_B(z) = z \otimes z \quad \& \quad [m]z = z^m \quad \forall\, m \in \mathbb{F}_p$$

The augmentation ideal I is $B(z-1) =$

$$\Lambda(z-1) + \cdots + \Lambda(z^{p-1} - 1)$$

For $i \in \mathbb{Z}$,

- $$y_i := (p-1)\, e_i\, (1-z) = \sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m)\,(1 - z^m)$$

  Depends only on i mod $p-1$

- $$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m)\, y_i \qquad \text{for } m \in \mathbb{F}_p^*$$

- $$S y_i = y_i \otimes 1 + 1 \otimes y_i + \frac{1}{1-p} \sum_{j=1}^{p-1} y_j \otimes y_{i-j}$$

$$I = \Lambda y_1 + \cdots + \Lambda_{p-1}$$

$$I_i = e_i I = \sum_j \Lambda y_j e_i \underset{\uparrow}{=} \Lambda y_i$$

$y_i = (p-1) e_i (1-z)$

Let $y := y_1$, gen of I_1

Let $w_1, w_2, w_3, \ldots$ be s.t.

$$I_i \ni y^i = w_i y_i \qquad \left(I_1^{\,i} = I_i \text{ for } i \in [1, p-1] \right)$$

$\therefore$ for $i \in [1, p-1]$, w_i is a unit

Proposition :

- w_i are invertible in Λ for $1 \le i \le p-1$. ✓
- $B = \Lambda[y]$ with $y^p = w_p y$ ✓
- $$s y = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_i \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$$ ✓
- $[m] y = \chi(m) y$ for $m \in \mathbb{F}_p$ ✓
- $w_i \equiv i! \pmod p$ for $1 \le i \le p-1$
- $$z = 1 + \frac{1}{1-p}\left(y + \frac{y^2}{w_2} + \cdots \frac{y^{p-1}}{w_{p-1}} \right)$$
- $w_p = p\, w_{p-1}$

Write z mod p & $s_B(z) = z \otimes z$ in terms of $S_B(y)$ & compare terms

Choose an embedding $\Lambda_p \hookrightarrow K$ where K is some field containing a primitive p root of unity ζ

Extend $\Lambda \hookrightarrow K$ to $\Lambda[z] \to K$ by sending $z \mapsto \zeta$

Let $y_i \longmapsto \eta_i$ & $\eta = \eta_1$

$$\eta_{p-1} = \mathrm{Im}(y_{p-1}) = \sum_{m\in\mathbb{F}_p^*} \chi^{-(p-1)}(m)\,(1-\zeta^m)$$

$$= \underbrace{p-1 \; - \sum_{m\in\mathbb{F}_p^*} \zeta^m}_{\shortparallel\; 0}$$

$$= p$$

$$\eta^{p-1} = \underbrace{w_{p-1}\,\eta_{p-1}}_{\neq 0} \qquad \therefore \quad \eta \neq 0$$

$$p\,w_{p-1} = \eta_{p-1}\,w_{p-1} = \eta^{p-1} = \frac{\eta^p}{\eta} = w_p$$

(Rmk: Using this embedding above we can compute $w_i \in \Lambda$ inductively)

Now, consider $\mathrm{Sym}^\bullet(\mathcal{J}_1) = \mathcal{O}_S \oplus \mathcal{J}_1 \oplus \mathrm{Sym}^2(\mathcal{J}_1) \oplus \cdots$

$\exists$ an $\mathcal{O}_S$-alg hom $\mathrm{Sym}^\bullet(\mathcal{J}_1) \xrightarrow{\varphi} \mathcal{A}$ induced by the inclusion $\mathcal{J}_1 \subset \mathcal{A}$

By the fact that $\mathcal{J}_1^i = \mathcal{J}_i$ $\forall\, i \in [1, p-1]$, this map is surjective.

Let $a \in \Gamma(S, \mathcal{J}_1^{\otimes 1-p})$ be the homomorphism $\mathcal{J}_1^{\otimes p} \longrightarrow \mathcal{J}_1$ induced by $\bullet$ in $\mathcal{A}$

$\ker\varphi$ is the ideal gen by $(a-1) \otimes I_1^{\otimes p}$

Let $G' = \operatorname{Spec} A'$ be the Cartier dual of G & let $\mathcal{J}'$, $\mathcal{J}'_i$ and $a' \in \Gamma(S, (\mathcal{J}'_i)^{\otimes 1-p})$ be the analogs of $\mathcal{J}$, $\mathcal{J}_i$ & a for G.

- Note that $(\mathcal{J}_A)' = \mathcal{J}_{A'}$

  as we are dualizing $\mathcal{O}_S \xrightarrow{e} \mathcal{O}_S \oplus \mathcal{J}_A \xrightarrow{\varepsilon} \mathcal{O}_S$

- $(\mathcal{J}_i)' = (e_i \mathcal{J})' = (\mathcal{J}')_i$

  $\mathcal{J}'_i = \{\varphi : [m]\varphi = \chi^i(m)\varphi\}$

  If $\varphi \in (e_i \mathcal{J})'$ $\quad ([m]\varphi)(a) = \varphi([m]a)$

  $$= \begin{cases} \chi^i(m)\,\varphi(a) & \text{if } a \in e_i\mathcal{J} \\ 0 & \text{if } a \in e_j\mathcal{J} \end{cases}$$

  $\therefore [m]\varphi = \chi^i(m)\varphi$

  $(e_i \mathcal{J})' \subseteq$

  $\vdots$

-