G: finite flat of order p

(Not quite) A Recap :

- Let S be a $\mathbb{Z}_p$ scheme. If G/S = Spec $\mathcal{A}$ then $\mathcal{A}$

2) $\cong \mathcal{O}_S \oplus \underbrace{\mathcal{I} \oplus \mathrm{Sym}^2\mathcal{I} \oplus \cdots \oplus \underbrace{\mathrm{Sym}^{p-1}\mathcal{I}}_{\mathcal{I}^{\otimes p-1}}}_{\text{augmentation ideal}}$ for an invertible sheaf $\mathcal{I}$

Alg structure comes from a map $a: \mathcal{I}^{\otimes p} \longrightarrow \mathcal{I}$
$a \in (\mathcal{I}^\vee)^{\otimes p-1}$

- $\mathcal{A}' \cong \mathcal{O}_S \oplus \mathcal{I}^\vee \oplus (\mathcal{I}^\vee)^{\otimes 2} \oplus \cdots \oplus (\mathcal{I}^\vee)^{\otimes p-1}$

w/ alg structure given by $b: \mathcal{I}^{\vee \otimes p} \longrightarrow \mathcal{I}^\vee$, $b \in (\mathcal{I})^{\otimes p-1}$

- Over $\mathbb{Z}_p$, $G = \mu_p$ = Spec A where

3) $A = \dfrac{\mathbb{Z}_p[y]}{y^p = w_p y}$ Here $w_p = \underbrace{w_{p-1}}_{\text{unit}} \cdot p$

$A' = \dfrac{\mathbb{Z}[y']}{y'^p = y'}$

- Recall : $G \times G' \longrightarrow \mathbb{G}_m$ nondegenerate
$\nearrow \mu_p \nearrow$
$\because G$ & G' are p-torsion

From this, it turns out that

$$\begin{array}{ccc} a \otimes b & \in & (\mathcal{I}^\vee)^{\otimes p-1} \otimes (\mathcal{I}^{\otimes p-1}) \\ \downarrow & & \wr\!\!\downarrow s \\ w_p & \in & \mathcal{O}_S \end{array}$$

- Theorem : For S over Spec $\mathbb{Z}_p$

1) {isom classes of S-gps of order p} $\longleftrightarrow$ {isom classes of triples (L, a, b) where L is an inv $\mathcal{O}_S$ sheaf, $a \in \Gamma(S, L^{\otimes p-1})$ $b \in \Gamma(S, L^{\otimes 1-p})$ & $a \otimes b = w_p \cdot I_{\mathcal{O}_S}$

injective, obvious

$G \longmapsto (\mathcal{I}^\vee, a, b)$

define using 2) define using 3)

$G^L_{a,b} \quad \longleftarrow\!\!| \quad (L, a, b)$

construct inverse using structure of μ_p

Locally on $S = \operatorname{Spec} R$, $\quad G^L_{a,b} = G \otimes_{R_0} R \quad$ where

- $R_0 = \mathbb{Z}_p[X_1, X_2]/X_1X_2 - w_p$
- $R_0 \longrightarrow R$
  $X_1 \longmapsto a$
  $X_2 \longmapsto b$
- $G = \operatorname{Spec} \dfrac{R_0[Y]}{Y^p = X_1 Y}$

$$sY = 1 \otimes Y + Y \otimes 1 + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{u^{p-1}}{w_i w_{p-i}} Y^i \otimes Y^{p-i}$$

E.g.

the only invertible sheaf

$$\mu_p/\mathbb{Z}_p \longleftrightarrow G^{\mathbb{Z}_p}_{w_p, 1}$$

$$\mu_p^\vee/\mathbb{Z}_p = \underline{\mathbb{Z}/p\mathbb{Z}}_{\mathbb{Z}_p} \longleftrightarrow G^{\mathbb{Z}_p}_{1, w_p}$$

$G^L_{a,b} \cong G^L_{a',b'} \iff \exists\, u \in \Gamma(S, \mathcal{O}_S^\times)$

$L \xrightarrow{\sim} L$

gen $\longmapsto$ $u \cdot$ gen

$a \longmapsto u^{p-1} a = a'$

$b \longmapsto u^{1-p} b = b'$

Digression : Étale fundamental gp :

Let S be connected & α a geometric pt of S

$$F : \text{Finite étale}/S \longrightarrow \text{finite sets}$$

$$\begin{array}{c} Y \\ \downarrow \pi \\ S \end{array} \longmapsto \pi^{-1}\alpha \cong \mathrm{Hom}_S(\alpha, Y)$$

$\pi(S) = \mathrm{Aut}\, F$ "étale fundamental gp of S"

We have a categorical equivalence : $F : \text{Finite étale}/S \xrightarrow{\sim}$ finite sets w/ cont. π-action

Finite étale gp schemes$/S \xrightarrow{\sim}$ finite π-modules

Finite étale gp schemes of order $p/S \xrightarrow{\sim}$ π-modules of order p $\xrightarrow{\sim}$ $\{$characters $\psi : \pi \longrightarrow \mathbb{F}_p^*\}$

E.g.

for K a field, $\pi(\mathrm{Spec}\, K) = \mathrm{Gal}(\bar{K}/K)$

for R integrally closed domain, $K = \mathrm{Frac}\, R$ $\quad \pi(\mathrm{Spec}\, R) = \bigcup \mathrm{Gal}(L/K)$

L/K finite, sep & integral closure of R in L is unramified over R

$\pi(\mathrm{Spec}\, \mathbb{Z}_p) = G_{\mathbb{Q}_p}^{un}$

Étale case : $G^L_{a,b}$ is étale over S, $S/\mathbb{Z}_p$

$\Leftrightarrow$ Locally on $\operatorname{Spec} R \subset S$, $G^R_{a,b} = \operatorname{Spec} \overbrace{\dfrac{R[y]}{y^p - ay}}^{A}$

$$\Omega_{G/R} = \frac{A\,dy}{(py^{p-1} - a)\,dy}$$

étale $\Leftrightarrow$ $\Omega = 0$ at each $k(x)$ $\Leftrightarrow (py^{p-1} - a) \neq 0$ in $k(x)$

$\Leftrightarrow \begin{cases} \overline{py} = 0 : & \bar{a} \neq 0 \\ \overline{py} \neq 0 & \bar{y}^p = \overline{ay} \Rightarrow \bar{a} = \bar{y}^{p-1} \neq 0 \end{cases}$

$k(py^{p-1} - a) = \underbrace{(p-1)}_{\text{unit}} \bar{y}^{p-1} \neq 0$

$\Leftrightarrow$ a is invertible

As $a \otimes b = w_p$, b is unique determined

Let $\alpha = \operatorname{Spec} \Omega$, geom pt of S

For étale $G^L_{a,b}$, $F(G^L_{a,b}) = \operatorname{Hom}_S(\alpha, G^L_{a,b})$

$G^L_{a,b} = \operatorname{Spec} \mathcal{O}_S \oplus \mathcal{J} \oplus \mathcal{J}^{\otimes 2} \oplus \cdots$

$= \{ x \in \operatorname{Hom}_{\mathcal{O}_S\text{-mod}}(\mathcal{J}, \Omega)$ $= \mathcal{J}^\vee \otimes \Omega$

satisfying $x^{\otimes p} = a \otimes x \}$

p choices for x : $x = 0$

or the $p-1$ sections x

satisfying $x^{\otimes p-1} = a$

Denote such a section by $\sqrt[p-1]{(a, L)}$

π acts on $G^L_{a,b}(\alpha)$ via ψ $\Rightarrow$ induces action on x

The attached Galois character satisfies

$$\left(\sqrt[p-1]{(a, L)}\right)^\sigma = \chi(\psi(\sigma)) \sqrt[p-1]{(a, L)}$$

$$\therefore \quad \psi(\sigma) = \chi^{-1}\left(\frac{\sqrt[p-1]{(a, L)}^{\,\sigma}}{\sqrt[p-1]{a, L}} \right)$$

Groups of order p over rgs of integers in # fields.

$K/\mathbb{Q}$ finite

R integrally closed $\subset K$, $\operatorname{Frac} R = K$

Let M = non generic pts of $\operatorname{Spec} R$ = nontriv discrete valuations of K whose val rg $\supset R$

For $v \in M$,

R_v = completion of R at v
K_v = $\operatorname{Frac} R_v$

Key idea:
Let $E(X)$ = isom classes of X-gps of order p

$$\begin{tikzcd}
E(R) \arrow[r] \arrow[d] & \prod_{v \in M} E(R_v) \arrow[d] \\
E(K) \arrow[r] & \prod_{v \in M} E(K_v)
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, mapsto] \arrow[d, mapsto] & \prod G \otimes R_v \arrow[d] \\
G \otimes K \arrow[r, mapsto] & \prod G \otimes K_v
\end{tikzcd}$$

is Cartesian.

To prove this we need a lemma:

Lemma: let G/S finite of order m. If m is invertible in $\mathcal{O}_S$, G is étale over S.

Pf: Finite, flat ✓

To check unramified, STS on geometric fibers.

(WTS that geo fibers are disjt unions of Spec k)

so let $S = \operatorname{Spec} k$, $k = \bar{k}$

Étale $\Leftrightarrow$ connected component of $e = G_0$ is trivial

($\because$ $\Rightarrow$ obv $\Leftarrow$: every connected component has a rational pt as these are finite type $k = \bar{k}$ schemes, & $G_0 = \operatorname{Spec} k$ $\Rightarrow$ by translation by rational pts, we get all conn. components are $\cong \operatorname{Spec} k$, $G = \operatorname{Spec} k \sqcup \cdots \sqcup \operatorname{Spec} k$)

If $G^\circ \neq \{e\}$, $G^\circ = \operatorname{Spec} A$, ($A$ is finite flat over k

Fact: order divides m

$\therefore \dim A = 0$ + finitely many irred components)

$\therefore$ A is a discrete set. By connectedness, 1 pt)

$\Rightarrow$ $A \overset{=}{} k \oplus I^{=m}$ is an artinian local rg with v.s. dim $= p$

$\Rightarrow$ $m \neq m^2$ $\Rightarrow$ $(m/m^2)^\vee \neq 0$

$\exists$ a k-derivation $d \neq 0$.

$d \in A'$

Leibniz rule gives $s_{A'}(d) = 1 \otimes d + d \otimes 1$

$k[d] \hookrightarrow A'$ is a Hopf subalg

Non triv. Map of gp schemes: $\operatorname{Spec} A' \longrightarrow \operatorname{Spec} k[d] \longrightarrow \operatorname{Spec} k[t] = \mathbb{G}_a$

order divides m

$d \longleftrightarrow d \longleftarrow t$

As the map is nontriv, not all closed pts go to e as closed pts are dense in A'

$\therefore \exists\, x^{\neq 0}$ in k, seen as im in $\mathbb{G}_a$ of a closed pt in A' s.t. $mx = 0$ $\Rightarrow x = 0$ $\Rightarrow\Leftarrow$

Back to our cartesian diagram

- Idea is where $v \nmid p$, or over K, it's étale, so we have a description in terms of π-modules
- where $v \mid p$, $\mathbb{Z}_p \subset R_v$ we have an explicit classification from prev section

Actually all we need for the applications is.

$$E(R) \hookrightarrow \prod E(R_v) \times_{\prod E(K_v)} E(K)$$

→ Certainly the map exists

If G, H are defined over R

s.t. $G \cong H$ over K & over all R_v

Then let $\varphi : G_K \xrightarrow{\sim} H_K$

$\Rightarrow \varphi_v : G_{K_v} \xrightarrow{\sim} H_{K_v}$

$\mathrm{Aut}(G_{R_v}) = \mathbb{F}_p^\times$

True for $v \nmid p$, $\because p$ invertible $\Rightarrow$ étale $\Rightarrow$ $\mathbb{F}_p^\times$ characters of π

For $v \mid p$, $\mathbb{Z}_p \subset R_v$, so our classification applies & we can check.

φ_v is coming from something over R_v by equal cardinalities of Aut gps.

So φ defined over R_v, K

$\therefore$ over R

Let $X =$ $\operatorname{Spec} K_v$ for any v or $\operatorname{Spec} R_v$ for $v \nmid p$ or $\operatorname{Spec} K$

As p is invertible on X

$$E(X) = \operatorname{Hom}_{cont}(\pi^{ab}(X), \mathbb{F}_p^*)$$

Class field theory:

$$\begin{array}{ccccc}
K^* \backslash \mathbb{A}^* = C_K & \longrightarrow & \pi(K)^{ab} & = & G_K^{ab} \\
\uparrow & & \uparrow & & \\
K_v^* & \longrightarrow & \pi(K_v)^{ab} & = & G_{K_v}^{ab} \\
\downarrow & & \downarrow & & \\
K_v^*/U_v & \longrightarrow & \pi(R_v)^{ab} & = & G_{K_v}^{un}
\end{array}$$

These homomorphisms become isom after passage to profinite completions of domains.

$$E(K) = \operatorname{Hom}_{cont}(C_K, \mathbb{F}_p^*)$$

$$E(K_v) = \operatorname{Hom}_{cont}(K_v^*, \mathbb{F}_p^*) \quad \forall v$$

$$E(R_v) = \operatorname{Hom}_{cont}(K_v^*/U_v, \mathbb{F}_p^*) \quad v \nmid p$$

Lemma

- Let $v | p$. Let $a \in K_v^*$, & let $\varphi_a \in \operatorname{Hom}_{cont}(K_v^*, \mathbb{F}_p^*)$ be the character corresponding to $G_{a,b}^{K_v}$ over K_v

Then $(a, x)_v := \varphi_a(x) = \dfrac{\sigma_x \beta}{\beta} \bmod m_v$ where $\beta^{p-1} = a$, $\sigma_x \in G_K^{ab}$ corresponding to x

& $\varphi_a(u) = \left(N_{R_v/\mathbb{F}_p}(\bar{u})\right)^{-v(a)}$ for $u \in U_v$

Fact: This pairing is non-deg bilinear on $K_v^*/K_v^{*p-1} \times K_v^*/K_v^{*p-1} \longrightarrow \mathbb{F}_p^*$

Claim ;
These conditions describe an elt of fiber product $E(R) \times_{\prod E(K_v)} \prod E(R_v)$

Theorem 3 :

$$\left\{ \begin{array}{c} \text{Isomorphism classes} \\ \text{of } R\text{-gps of order } p \end{array} \right\} \hookrightarrow \left\{ \begin{array}{l} (\psi, (n_v)_{v|p}) \text{, where } \psi : C_K \to \mathbb{F}_p^{\times}, \\ 0 \le n_v \le v(p) \quad \forall v|p \text{ and the} \\ \text{following conditions are satisfied :} \\ \text{(i) for } v \nmid p \quad \psi \text{ is unramified at } v \\ \qquad \Leftrightarrow \psi_v(U_v) = 1 \\ \text{(ii) for } v|p, \quad \psi_v(u) = (N_{k_v/\mathbb{F}_p}(\bar{u}))^{-n_v} \\ \qquad \forall u \in U_v \end{array} \right\}$$

actually bijection

(Here $\psi_v : K_v^{\times} \to C_K \xrightarrow{\psi} \mathbb{F}_p^{\times}$)

$$G \longmapsto (\varphi^G, (n_v^G)_{v|p})$$

where φ^G is the idèle class character determined by $G \otimes_R K$

For $v|p$, $G \otimes_R R_v \cong G_{a, w_p a^{-1}}^{R_v}$

$0 \le n_v^G := v(a) \le v(w_p) = v(p)$

- For $v \nmid p$, Condition (i) is saying that ψ_v should be coming from the generic fiber of a unique gp scheme over R_v $\Leftrightarrow$ $E(R_v) \to \psi_v \in E(K_v)$

  Clear

  i.e. fiber over ψ_v contains exactly 1 elt

- For $v|p$, Condition (ii) guarantees that fiber over $\psi_v \in E(K_v)$ is non-empty in $E(R_v) \to E(K_v)$

  Furthermore it is unique if we restrict consideration to $G_v \cong G_{a, w_p a^{-1}}^{R_v}$ in preimage s.t. $v(a) = n_v$

Pf : If $G_v = G^{R_v}_{a, w_p a \tau}$ is in preimage of Ψ_v, then

$\Psi_v = \varphi_a$ by prev lemma

$K_v^* / (K_v^*)^{p-1} \xrightarrow{\sim} \mathrm{Hom}_{gp}(K_v^* / (K_v^*)^{p-1}, \mathbb{F}_p^*)$ (by non degeneracy of $(a, x)_v := \varphi_a(x)$)

$\therefore \exists$ a unique $a \in K_v^*$ mod $(K_v^*)^{p-1}$ s.t. $\varphi_a = \Psi_v$

By prev lemma $\varphi_a(u) = N_{k_v/\mathbb{F}_p}(\bar{u})^{-v(a)}$

As $N_{k_v/\mathbb{F}_p}$ is surjective, $n_v \equiv v(a) \mod p-1$

Changing a by a $p-1$ power of uniformizer, we get $v(a) = n_v$ & a uniquely determined mod $K_v^{p-1} \cap U_v =$ mod U_v^{p-1}

$\therefore G_v$ is uniquely determined.

Note that
For a given family of integers $(n_v)_{v|p}$,

- either there is no idèle class char satisfying (i) & (ii), or
- the set of all such has a free & transitive action by the gp of characters $\underbrace{k^\times \backslash \mathbb{A}^\times / \prod U_v}_{\text{ideal class gp}} \longrightarrow \mathbb{F}_p^\times$

$\therefore$ If class number is prime to p, $\exists$ at most one ψ for each family $(n_v)_{v|p}$

$\#$ of families $(n_v)_{v|p} = \prod_{v|p} \underbrace{(v(p)+1)}_{\text{choices } 0 \le n_v \le v(p)}$.

$\therefore$ if p is prime in R, $\exists$ just 2 families : $n_v = 0$, $n_v = 1$ for the unique $v|p$

Corollary: If $R = \mathbb{Z}$ or if R is rg of integers in a field of class # prime to $p-1$ s.t pR is a prime ideal in R, then the only R-gps of order p are $(\mathbb{Z}/p\mathbb{Z})_R$ & $\mu_{p,R}$

Corollary: Let R be a rg of integers in a field of ramification index $< p-1$ at all places above p. Then a gp scheme over R of order p is determined by its generic fibers.

Pf: Generic fiber determines ψ_v satisfying (i) & (ii) $\forall v$

- for $v \nmid p$, we get a unique elt of $E(R_v)$ giving ψ_v in its generic fiber
- For $v | p$, we found G_v earlier by finding a: $\varphi_a = \psi_v$

As $v(a) < p-1$ $\because$ $v(p) < p-1$.
knowing $\psi_v(u)$ determines n_v mod $p-1$
& $\therefore$ $v(a)$ is determined
$\therefore$ a is determined mod U^{p-1}.