A crash course in $\star$ cohomology

$\star \in \{$Zariski, étale, fppf$\}$

Fix a base scheme S.

We should define $\star$ sheaves over S. Luckily, we just need representable ones.

"Def" A representable $\star$ sheaf of abelian groups over S is simply a group scheme $G \to S$, with G abelian.

Why "sheaves"? Let $T \xrightarrow{f} S$ be a scheme morphism. Suppose that f is:

- an open immersion, if $\star = \mathrm{Zar}$
- an étale map, if $\star = \text{étale}$
- a flat map of finite presentation, if $\star = \mathrm{fppf}$

Then we define $\mathcal{G}(T \to S)$ simply as $\mathcal{G}_T(T)$

$$\begin{tikzcd} \mathcal{G}_T \arrow[r] \arrow[d] \arrow[dr, phantom, very near start, "\lrcorner"] & \mathcal{G} \arrow[d] \\ T \arrow[r] \arrow[ur, dashed] & S \end{tikzcd}$$

Main examples

- $\mathcal{G} = \mu_{n,S} = \mu_{n,\mathbb{Z}} \times_{\operatorname{Spec}\mathbb{Z}} S \qquad \mu_{n,\mathbb{Z}} = \dfrac{\mathbb{Z}[x]}{(x^n - 1)}$

$$\mathcal{G}(T) = \{ \zeta \in \mathcal{O}_T(T)^\times \mid \zeta^n = 1 \}$$

$$\begin{tikzcd}
\mu_{n,T} \arrow[r] \arrow[d] & \mu_{n,S} \arrow[r] \arrow[d] & \mu_{n,\mathbb{Z}} \arrow[d] \\
T \arrow[r] \arrow[u, dashed, bend left] \arrow[urr, dashed] & S \arrow[r] & \operatorname{Spec} \mathbb{Z}
\end{tikzcd}$$

$$\mathrm{Hom}_{Sch}(T, \mu_{n,\mathbb{Z}}) = \mathrm{Hom}_{Ring}\left(\frac{\mathbb{Z}[x]}{(x^n-1)}, \mathcal{O}_T(T) \right) = \{ \zeta \in \mathcal{O}_T(T)^\times \mid \zeta^n = 1 \}$$

- $\mathcal{G} = \mathbb{G}_{m,S}$ $\qquad\qquad$ $\mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[x, \frac{1}{x}]$

  $\mathbb{G}_m(T) = \mathcal{O}_T(T)^\times$

- $\mathcal{G} = (\mathbb{Z}/p\mathbb{Z})_S$ $\qquad\qquad$ $(\mathbb{Z}/p\mathbb{Z})_{\mathbb{Z}} = \mathbb{Z}^p$ with suitable multiplication.

  $\mathcal{G}(T) = (\mathbb{Z}/p\mathbb{Z})^{\# \text{ connected components of } T}$

The notion of exact sequence

$$0 \to \mathcal{G}' \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{G}'' \longrightarrow 0 \quad \text{sheaves over } S.$$

Exactness: for every $T \to S$ of type $\star$ and every $g \in \mathcal{G}(T)$ such that $\beta(g) = 0$, $\exists\ T_1 \to T \to S$ of type $\star$ and $h \in \mathcal{G}'(T_1)$ s.t. $\alpha(h) = g$.

Ex $\quad 1 \to \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{\wedge n} \mathbb{G}_m \longrightarrow 1$ over $\operatorname{Spec} \mathbb{Z}$

(i) • Not exact in Zar

(ii) • Not exact in ét (hard-ish); exact over $\operatorname{Spec} \mathbb{Z}[1/n]$

(iii) • Exact in fppf

(i). Take $T \to S$ to be $\operatorname{Spec} \mathbb{Z}[1/p] \hookrightarrow \operatorname{Spec} \mathbb{Z}$.

Then $\mathbb{G}_m(T) = \mathbb{Z}[1/p]^* \ni p$. But there is no open subscheme of T over which p becomes an n-th power.

(iii) [Example] Take $p \in \mathbb{G}_m(T)$ as above. Take

$$T_1 = \operatorname{Spec} \mathbb{Z}[1/p][y]/(y^n - p)$$

This is flat (even free!) over $T = \operatorname{Spec} \mathbb{Z}[1/p]$, and $y \in \mathbb{G}_m(T_1)$, so $p = y^n$ over T_1

(ii) [Example] Note that $T_1 \to T$ is flat but NOT étale!

But it is étale if we invert n.

Long Exact Sequence in cohomology

Given $0 \to \mathcal{G}_1 \to \mathcal{G} \to \mathcal{G}_2 \to 0$ exact in the $\star$-topology,

we get $0 \to \mathcal{G}_1(S) \to \mathcal{G}(S) \to \mathcal{G}_2(S) \to H^1_\star(S, \mathcal{G}_1) \to H^1_\star(S, \mathcal{G})$

$\to H^1_\star(S, \mathcal{G}_2) \to H^2(S, \mathcal{G}_1) \to \dots$

Facts

Dedekind domain

(i) $S = \operatorname{Spec} R$, $\quad H^1_\star(S, \mathbb{G}_m) = Cl(R)$

(ii) More generally, $H^1_\star(S, \mathbb{G}_m) = \operatorname{Pic}(S)$

(iii) $H^1_\star(\operatorname{Spec} \mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = (0)$

Cor $H^1_{fppf}(\mathbb{Z}, \mu_n) = ?$

Proof $1 \to \mu_n \to \mathbb{G}_m \xrightarrow{\wedge n} \mathbb{G}_m \to 1$ is exact in fppf.

$$\Rightarrow \quad H^0(S, \mathbb{G}_m) \longrightarrow H^0(S, \mathbb{G}_m) \longrightarrow H^1(S, \mu_n)$$
$$\longrightarrow H^1(S, \mathbb{G}_m) \xrightarrow{\wedge n} H^1(S, \mathbb{G}_m)$$

$$\{\pm 1\} \xrightarrow{\wedge n} \{\pm 1\} \longrightarrow H^1(S, \mu_n) \longrightarrow 0$$

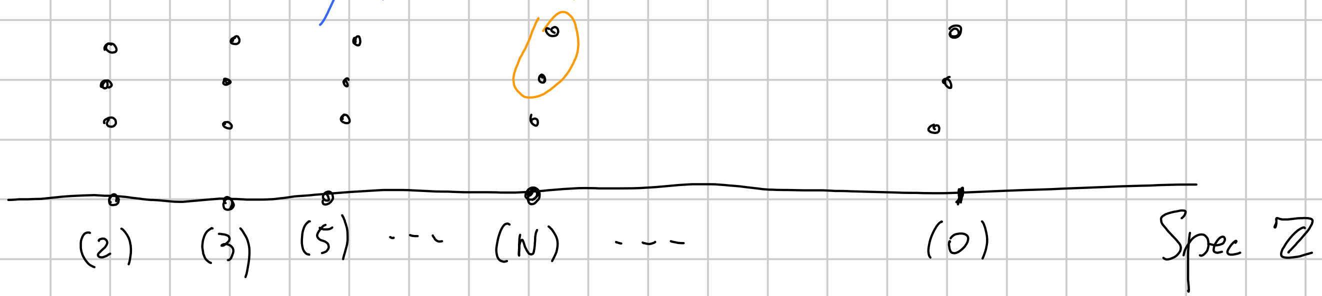
$$\Rightarrow \quad H^1(S, \mu_n) \simeq \frac{\{\pm 1\}}{\{(\pm 1)^n\}} \simeq \begin{cases} \text{trivial}, & n \text{ odd} \\ \mathbb{Z}/2\mathbb{Z}, & n \text{ even} \end{cases}$$

— later —

The groups $(\mathbb{Z}/p\mathbb{Z})^b$ and μ_p^b

erase this

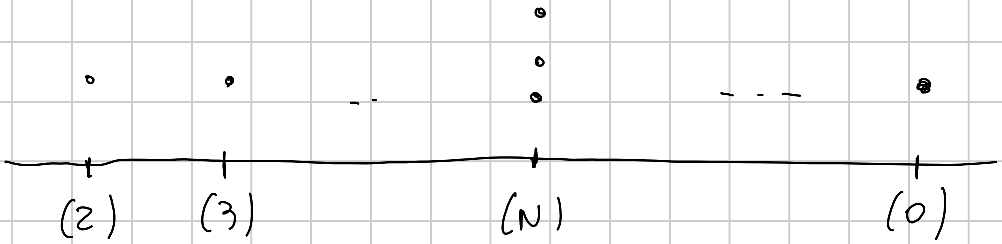
$(\mathbb{Z}/p\mathbb{Z})^b$:



$$H^0\left(\operatorname{Spec}\mathbb{Z},\ \left(\mathbb{Z}/p\mathbb{Z}\right)^b\right) = (0)$$

$$0 \to \left(\mathbb{Z}/p\mathbb{Z}\right)^b \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow G \longrightarrow 0$$

G :



Proof of weak Mordell-Weil via étale / fppf cohomology

A/K ab. var. We want to show that $\frac{A(K)}{nA(K)}$ is finite.

It suffices to do so after finite Galois extension. Indeed, from

$$0 \to A[n](L) \to A(L) \to [n]A(L) \to 0$$

we get $A(K) \xrightarrow{[n]} [n]A(L) \cap A(K) \to H^1(G, A[n](L))$,

which gives the finiteness of $\frac{[n]A(L) \cap A(K)}{[n]A(K)}$.

OTOH, from $0 \to [n]A(L) \to A(L) \to \frac{A(L)}{[n]A(L)} \to 0$ we get

$$[n]A(L) \cap A(K) \to A(K) \to (\text{finite}),$$

$\longrightarrow$ weak M-W over L

which shows that

$$\left| \frac{A(K)}{[n]A(L) \cap A(K)} \right| < +\infty$$

Combined with $\left| \frac{[n]A(L) \cap A(K)}{[n]A(K)} \right| < +\infty$, this concludes.

So, back to wmlw over L s.t. $A[n](L) = A[n](\overline{K})$.
Extend A to ab. sch. over $R := \mathcal{O}_K[\frac{1}{N}]$. I claim that

$$0 \to \mathcal{A}[n] \to \mathcal{A} \xrightarrow{[n]} \mathcal{A} \to 0$$

is exact in the fppf topology. Assuming this,

$$\mathcal{A}(R) \xrightarrow{[n]} \mathcal{A}(R) \to H^1_{fppf}(R, \mathcal{A}[n]),$$

hence $\dfrac{A(K)}{[n]A(K)} \hookrightarrow H^1_{fppf}(R, \mathcal{A}[n])$

But $\mathbb{G}_m(R) \xrightarrow{\wedge n} \mathbb{G}_m(R) \longrightarrow H^1_{fppf}(R, \mathcal{A}[n]) \to Cl(R) \xrightarrow{[n]} Cl(R)$,

so $R^\times / R^{\times n} \longrightarrow H^1_{fppf}(R, \mathcal{A}[n]) \longrightarrow Cl(R)[n]$, and

the finiteness follows from finite generation of $R^\times$ (gener. Dirichlet) + finiteness $Cl(R)$ ($\Leftarrow$ finiteness $Cl(\mathcal{O}_K)$).

The real stuff: "Theorem B" in Snowden's notes

<u>Thm</u> Let $A/\mathbb{Q}$ be an ab. variety. Suppose there exist two primes $p \nmid N$ such that

- A has good red outside N
- A " totally toric red at N
- the finite gp scheme $A[p] / \operatorname{Spec} \mathbb{Q}$ is an iterated extension of $\mathbb{Z}/p\mathbb{Z}$'s and μ_p's. More concretely: the J-H consituents of $A[p](\bar{\mathbb{Q}})$ are $\mathbb{Z}/p\mathbb{Z}$ or μ_p.

Then $\operatorname{rk} A(\mathbb{Q}) = 0$.

Idea Extend A to its Néron model $\mathcal{A}$ over $\mathbb{Z}$. We have an exact sequence (in the fppf topology)

$$0 \to \mathcal{A}^\circ[p^n] \longrightarrow \mathcal{A}^\circ \xrightarrow{[p^n]} \mathcal{A}^\circ \longrightarrow 0,$$

hence

$$\frac{\mathcal{A}^\circ(\mathbb{Z})}{p^n\mathcal{A}^\circ(\mathbb{Z})} \hookrightarrow \underbrace{H^1_{fppf}(\mathbb{Z}, \mathcal{A}^\circ[p^n])}_{\text{we'll show that the order of this stays BOUNDED as } n \text{ varies.}}$$

It follows that $\mathcal{A}^\circ(\mathbb{Z}) \subseteq \mathcal{A}(\mathbb{Z}) = A(\mathbb{Q}) = \mathbb{Z}^r \oplus T$ is fin. gen., and in fact of rank zero. But

$$0 \to \mathcal{A}^\circ \to \mathcal{A} \to C \to 0 \quad \text{with } C \text{ finite, so}$$

$$0 \to \mathcal{A}^\circ(\mathbb{Z}) \to \mathcal{A}(\mathbb{Z}) = A(\mathbb{Q}) \longrightarrow C(\mathbb{Z})$$

shows that $A(\mathbb{Q})$ is finite, as desired.

So "all" we have to do is show that

$$\# H^1_{fppf}(\operatorname{Spec} \mathbb{Z}, \mathcal{A}^\circ[p^n])$$

stays bounded. Note that $\# H^0(\mathbb{Z}, \mathcal{A}^\circ[p^n]) \leq \# \mathcal{A}^\circ(\mathbb{Z})_{tors}$
$\leq \# \mathcal{A}(\mathbb{Z})_{tors} = A(\mathbb{Q})_{tors}$ is uniformly bounded,
so it would suffice to show that $\# H^1 / \# H^0$ is bounded.

Convention From now on, all gp schemes are killed by p^n for some n. This implies that $H^0(\mathbb{Z}, G)$ and $H^1(\mathbb{Z}, G)$ are p-grps. Set $h^0(G) := \log_p \# H^0(\mathbb{Z}, G)$, $h^1(G) := \log_p \# H^1(\mathbb{Z}, G)$

Lemma Let $0 \to G_1 \longrightarrow G \longrightarrow G_2 \longrightarrow 0$ be a SES of gp schemes over $\mathbb{Z}$. We have

$$(h^1 - h^0)(G) \leq (h^1 - h^0)(G_1) + (h^1 - h^0)(G_2).$$

Proof Write out long ex. seq.

$$0 \to H^0(G_1) \to H^0(G) \to H^0(G_2) \to H^1(G_1) \to H^1(G) \to H^1(G_2) \to C \to 0$$

$$\frac{\# H^0(G_1) \cdot \# H^0(G_2) \cdot \# H^1(G) \cdot \# C}{\# H^0(G) \cdot \# H^1(G_1) \cdot \# H^1(G_2)} = 1$$

Taking $\log_p$,

$$(h^0 - h^1)(G_1) + (h^0 - h^1)(G_2) + (h^1 - h^0)(G) + \log_p \# C = 0$$

$$\Rightarrow \quad (h^1 - h^0)(G) = (h^1 - h^0)(G_1) + (h^1 - h^0)(G_2) - \log_p \# C \qquad \square$$

So: we want $h^1(\mathbb{Z}, \mathcal{A}^\circ[p^n])$ bounded; equivalently, $(h^1 - h^0)(\mathcal{A}^\circ[p^n])$ bounded. Note that

$$0 \to \mathcal{A}^\circ[p] \longrightarrow \mathcal{A}^\circ[p^n] \xrightarrow{[p]} \mathcal{A}^\circ[p^{n-1}] \longrightarrow 0,$$

so by induction $(h^1 - h^0)(\mathcal{A}^\circ[p^n]) \leq n \cdot (h^1 - h^0)(\mathcal{A}^\circ[p])$

We'll show $(h^1 - h^0)(\mathcal{A}^\circ[p]) \leq 0$, which is certainly enough.

(Pre)admissible group schemes

From now on, fix N & p as in the statement of the main thm.

↝ claim that $G := \mathcal{A}^\circ[p]$ has the following properties:

1) the restriction to $\mathbb{Z}[1/N]$ is finite & flat

Key pt:

$$\begin{tikzcd} \mathcal{A}^\circ[p] \arrow[r] \arrow[d] & \mathcal{A}^\circ \arrow[d, "{[p]}"] \\ \{0\} \arrow[r] & \mathcal{A}^\circ \end{tikzcd}$$

over $\mathbb{Z}[1/N]$

projective + flat

↓

fibral criterion for flatness

2) this same restriction has a filtration

$$0 = F^0 G \subseteq F^1 G \subseteq F^2 G \subseteq \dots \subseteq F^n G = G$$

such that $F^{n+1}G/F^nG \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z} \\ \mu_p \end{cases}$ over $\mathbb{Z}[1/N]$

The proof is that over $\mathbb{Z}[1/pN]$ the scheme is étale, hence determined by its $\overline{\mathbb{Q}}$-pts. Extend over p by Raynaud (resp. Fontaine for $p=2$)

Fact There are 4 elementary admissible gps over $\mathbb{Z}$.
Their invariants

$$\alpha := \#\text{ of } \mathbb{Z}/p\mathbb{Z} \text{ in } (G)_{\mathbb{Z}[1/N]}, \qquad \delta := \log \# G_{\mathbb{Q}} - \log \# G_{\mathbb{F}_N}$$

are

	$\mathbb{Z}/p\mathbb{Z}$	$(\mathbb{Z}/p\mathbb{Z})^b$	μ_p	μ_p^b
δ	0	1	0	1
α	1	1	0	0
h^0	1	0	$\begin{cases} 0 & p \text{ odd} \\ 1 & p=2 \end{cases}$	0
h^1	0	0	$\begin{cases} 0 & p \text{ odd} \\ 1 & p=2 \end{cases}$	ε

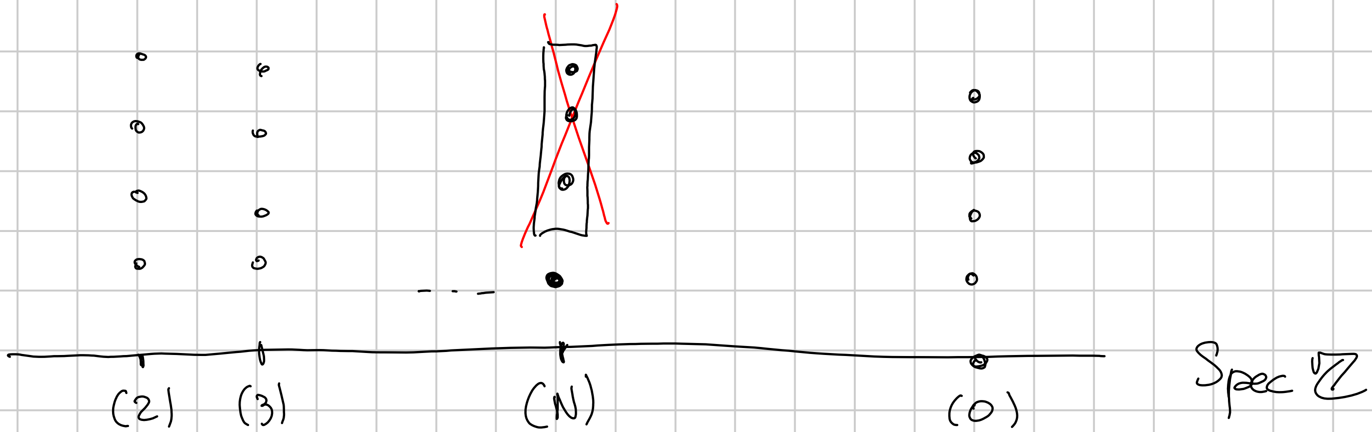
ε: 0 or 1

Lemma $h^1 - h^0 \leq \delta - \alpha$ for all admissible schemes

Pf LHS is sub-additive in SES, RHS is additive $\Rightarrow$ it suffices to check this for the elementary ones, and the table shows that it's true!

"Proof"

- Description of gps: $\mu_p^\flat$, $(\mathbb{Z}/p\mathbb{Z})^\flat$ look like this:



- h^1: let's start with $(\mathbb{Z}/p\mathbb{Z})^\flat$.

$$0 \to (\mathbb{Z}/p\mathbb{Z})^\flat \to \mathbb{Z}/p\mathbb{Z} \to \overset{(i_{\mathbb{F}_N})_*(\mathbb{Z}/p\mathbb{Z})}{C} \to 0$$

$$0 \to \underbrace{H^0(\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})}_{=\mathbb{Z}/p\mathbb{Z}} \xrightarrow{\sim} \underbrace{H^0(\mathbb{Z}, C)}_{=\mathbb{Z}/p\mathbb{Z}} \to \underbrace{H^1_{fppf}(\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^\flat)}_{=(0)}$$

$$C \longrightarrow H^1_{fppf}(\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = (0)$$

Now μ_p^b

$$1 \to \mu_p^b \longrightarrow \mu_p \longrightarrow C \longrightarrow 0$$

$$(0) \longrightarrow \mu_p(\mathbb{Z}) \longrightarrow \mu_p(\mathbb{F}_N) \longrightarrow H^1_{fppf}(\mathbb{Z}, \mu_p^b) \longrightarrow H^1_{fppf}(\mathbb{Z}, \mu_p)$$

* For $p \neq 2$: $\quad 0 \to \mu_p(\mathbb{F}_N) \xrightarrow{\sim} H^1_{fppf}(\mathbb{Z}, \mu_p^b) \longrightarrow 0$

$\hookrightarrow$ size $\begin{cases} p, & p \mid N-1 \\ 1, & p \nmid N-1 \end{cases}$

* For $p=2$: $\quad 0 \to \{\pm 1\} \to \underbrace{\{\pm 1\}}_{N \neq 2} \to H^1_{fppf}(\mathbb{Z}, \mu_p^b) \to \{\pm 1\}$,

hence it has order 1 or 2. In fact, it's the kernel of

↳ which is enough for our purposes anyway.

$$H^1_{fppf}(\mathbb{Z}, \mu_p) \to H^1_{fppf}(\mathbb{F}_N, \mu_p)$$

$$\left[\frac{\mathbb{Z}[x]}{(x^2+1)}\right] \longmapsto \left[\frac{\mathbb{F}_N[x]}{(x^2+1)}\right], \text{ trivial iff } N \equiv 1 \ (4)$$

So there's a kernel (hence $h^1(\mu_p^b) > 0$) if $N \equiv 1 \ (4)$