Groupes de type multiplicatif

Déf : Un k-groupe alg. affine G est de type mult. si $G_{\bar{k}}$ est diagonalisable.

th Soit G un k-groupe alg affine. LCSSE : ($k^s \subset \bar{k}$ clôture séparable)

(1) $G_{\bar{k}}$ est diagonalisable, ie G est de type mult

(2) G_{k^s} est diagonalisable.

Rem c'est tout à fait faux avec (par ex.) les groupes unipotents.
Par exemple $G = \{y^p = x - tx^p\} \subseteq \mathbb{G}_{a,k}$ où $t \in k \setminus k^p$ devient isomorphe à $\mathbb{G}_a$ après changement de base à $k(t^{1/p})$, mais pas après un changement de base séparable !

Dém Seule (1) $\Rightarrow$ (2) est à démontrer.
Par hypothèse il existe un iso $f : G_{\bar{k}} \longrightarrow D(M)_{\bar{k}}$. Celui-ci est donné par un morphisme d'algèbres de Hopf

$$\bar{k}[M] \longrightarrow \mathcal{O}(G) \otimes_k \bar{k}$$

qui à son tour est donné par les images des générateurs X^m pour m dans un syst. de générateurs du groupe abélien M.
Ces images s'écrivent $\sum_{\text{finie}} f_i \otimes \lambda_i$ avec $\lambda_i \in \bar{k}$ et sont en nb fini.
Soit $\ell \subset \bar{k}$ l'extension engendrée par les λ_i ; elle est finie sur k.
On a donc un iso ~~(il faut p.ê grossir un peu ℓ pour que ce soit un iso)~~ : $k[M] \otimes \ell \longrightarrow \mathcal{O}(G) \otimes \ell$.
Soit $F = \underline{\mathrm{Isom}}_{k\text{-gr}}(G, D(M))$ le foncteur des isomorphismes (semblable au foncteur d'automorphismes de l'exposé introductif), i.e $F(A) = \mathrm{Isom}_{A\text{-gr}}(G \otimes_k A, D(M) \otimes_k A)$ $\forall A/k$ k-algèbre.

$F : (k\text{-Alg}) \to \mathrm{Ens}.$

On vient de montrer que $F(\ell) \neq \emptyset$ pour une ℓ/k finie.

Alors $F \otimes_k \ell = \underline{\mathrm{Isom}}_{\ell\text{-gr}}(G_\ell, D(M)_\ell) \simeq \underset{\ell\text{-gr}}{\mathrm{Aut}}(D(M)_\ell) \simeq \underline{\mathrm{Aut}(M)}^0_\ell$

car $G_\ell \simeq D(M)_\ell$ — éq de cat $\{\text{diagonalisables}\} \leftrightarrow \{\text{gr ab TF}\}$

ici $\underline{\mathrm{Aut}(M)}^0_\ell = \coprod_{\mu \in \mathrm{Aut}(M)} \mathrm{Spec}(\ell)$ est le ℓ-groupe constant, représentable par un ℓ-schéma étale (mais p.ê infini i.e avec un ∞ de comp. connexes).

Dans ce contexte, le th B.26 de Milne (Appendice sur les quotients) montre que F lui-même est représentable par un k-schéma.

De plus il est « élémentaire » que $\left\| \begin{array}{l} F\otimes \ell \to \mathrm{spec}\, \ell \text{ étale} \\ \Rightarrow F \to \mathrm{Spec}\, k \text{ étale} \end{array}\right.$

donc $F = \underline{\mathrm{Isom}}_k(G, D(M)) = \coprod_{i\in I} \mathrm{spec}(k_i)$ ← ext. finie séparable de k.

Pour n'importe lequel des k_i on a un point $\mathrm{Spec}(k_i) \to F$ c'est-à-dire un k_i-isomorphisme $G_{k_i} \xrightarrow{\sim} D(M)_{k_i}$.

Comme $k_i \subset k^s$ on a gagné. $\boxtimes$

<u>Rem</u> Milne démontre ceci très différemment. Il montre :

LCSSE (a) $G_{\bar{k}}$ diagonalisable

(b) G commutatif et $\mathrm{Hom}(G, \mathbb{G}_a) = 0$

(c) G commutatif et $\mathcal{O}(G)$ est réunion filtrante de sous-coalgèbres à duale étale

(d) G_{k^s} diagonalisable.

(a) $\Rightarrow$ (b) vient de ce que si $\varphi \in \mathrm{Hom}(G, \mathbb{G}_a)$, $\varphi \neq 0$ alors

$g \mapsto \begin{pmatrix} 1 & \varphi(g) \\ 0 & 1 \end{pmatrix}$ est une rep. non semi-simple.

Le reste est plus technique...

Ce résultat permet une classification des groupes de type mult en termes de modules galoisiens, comme suit.

"Rappels" de théorie de Galois infinie — Neukirch, Algebraic Number theory chap IV

Prenons $k = \mathbb{F}_p$ et $K = \overline{\mathbb{F}}_p = \mathbb{F}_p^{sep} = \varinjlim_m \mathbb{F}_{p^m}$.

On a $\mathbb{F}_{p^m} = \{x \in \overline{\mathbb{F}}_p \,;\, x^{p^m} = x\} = (\overline{\mathbb{F}}_p)^{\varphi^m}$ où $\varphi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, $x \mapsto x^p$ le Frobenius.

Posons $\Gamma := Gal(\overline{\mathbb{F}}_p / \mathbb{F}_p)$.

La description ci-dessus de $\mathbb{F}_{p^m}$ montre qu'il est stable par tout élément $\sigma \in \Gamma$ d'où une flèche $\Gamma \to \varprojlim_{\substack{l/k \text{ finie} \\ l = \mathbb{F}_{p^m} \text{ ici!}}} Gal(l/k)$ qui est iso.

$$\sigma \mapsto (\sigma_{|l})$$

Comme $Gal(\mathbb{F}_{p^m}/\mathbb{F}_p) = \langle \varphi \mid \varphi^m = 1 \rangle \simeq \mathbb{Z}/m\mathbb{Z}$, il vient

$$\Gamma \xrightarrow{\sim} \varprojlim_m \mathbb{Z}/m\mathbb{Z} =: \widehat{\mathbb{Z}}.$$

Le th des restes chinois permet de décomposer selon les premiers et de voir que $\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$ $\quad \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ = entiers p-adiques.

Soit $H = \langle \varphi \rangle = \mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$ le sous-groupe engendré par φ.

On a $H \subsetneq \Gamma$ alors que $\overline{\mathbb{F}}_p^{\,\Gamma} = \overline{\mathbb{F}}_p^{\,H} = \mathbb{F}_p$ ce qui pose problème pour l'injectivité de la corresp. de Galois

$$\{\text{sous-groupes de } \Gamma\} \longrightarrow \{\text{sous-extensions de } K\}$$
$$H \longmapsto K^H$$

Idée on restaure la correspondance en se restreignant aux sous groupes d'indice fini. Si on les prend pour base des voisinages ouverts de $1 \in \Gamma$ (i.e : H ouvert $\overset{df}{\Longleftrightarrow} [\Gamma : H] < \infty$) on définit la topologie de Krull ou topologie profinie sur Γ.

Pour k quelconque et $K = k^{sep}$ on aura

$$\underset{\text{topologisé}}{\Gamma = Gal(K/k)} \xrightarrow{\sim} \varprojlim_{l/k \text{ finie galoisienne}} Gal(l/k)$$

et le th fondamental de la théorie de Galois devient :

<u>th</u> Soit k corps et $\Gamma = \mathrm{Gal}(k^{sep}/k)$. On a des bijections :

$$\begin{array}{ccc} \{\text{sous-groupes ouverts de } \Gamma\} & \longleftrightarrow & \{\text{sous-ext } l/k \text{ finies}\} \\ \cap & & \cap \\ \{\text{sous-groupes fermés de } \Gamma\} & \longleftrightarrow & \{\text{sous-ext } l/k \text{ qcq}\} \end{array} \quad \boxtimes$$

Rappelons aussi que les extensions inséparables n'ont pas d'automorphismes donc pas de théorie de Galois :

Si $k_0 = \mathbb{F}_p(t) \subset k = k_0(\alpha)$ avec $\alpha^p = t$,
le polynôme $X^p - t \in k_0[X]$ devient $X^p - \alpha^p = (X-\alpha)^p \in k[X]$
un $f \in \mathrm{Aut}(k/k_0)$ doit permuter les racines... donc $f = \mathrm{id}$!

C'est pourquoi on peut appliquer Galois $k \subset k^{sep} \subset \bar{k}$
ici ↑ ; ↑ inséparable

<u>Pour les groupes de type multiplicatif</u> ça marche comme ça.

Si G/k est de type mult alors $G_{k^s} \simeq D(M)$
où $M = \mathrm{Hom}_{k^s}(G_{k^s}, \mathbb{G}_{m,k^s})$ groupe des caractères. C'est un gr. ab muni d'une action de $\Gamma = \mathrm{Gal}(k^s/k)$ par pullback :

$$\begin{tikzcd}
G \arrow[r] \arrow[d] \arrow[rrd] & \mathbb{G}_m \arrow[ld] \arrow[rrd] & & \\
\mathrm{Spec}(k^s) \arrow[rrd, "\sigma"] & & G \arrow[r, "\chi"] \arrow[d] & \mathbb{G}_m \arrow[ld] \\
& & \mathrm{Spec}\, k^s &
\end{tikzcd}$$

On appelle ça un ($\mathbb{Z}$-) module galoisien.

De plus comme χ est défini sur une sous-ext finie l/k, l'action est continue i.e. chaque élément $\chi \in M$ a un stabilisateur ouvert i.e. d'indice fini :

$$M = \bigcup_{l/k \text{ finie}} M^{\mathrm{Gal}(l/k)}.$$

[<u>Exercice</u> : si M est discret on a équivalence : (1) $\Gamma \times M \to M$ continue (2) stab. de pts ouverts]

<u>th</u> on a une équiv de catégories : $\qquad \Gamma = \mathrm{Gal}(k^s | k)$

$$\{ k\text{-gr alg de type multiplicatif} \} \longleftrightarrow \left\{ \begin{array}{l} \text{modules galoisiens =} \\ \text{gr. ab. avec action} \\ \text{continue de } \Gamma \end{array} \right\}$$

$$G \longmapsto M = \mathrm{Hom}_{k^s}(G_{k^s}, \mathbb{G}_{m,k^s}) + \circlearrowleft \Gamma$$

$$\mathrm{Spec}\left(k[M]^{\Gamma}\right) \longleftarrow\!\shortmid M \qquad \boxtimes$$

<u>Exemple</u> un <u>tore</u> est un k-gr. de type mult. <u>lisse connexe</u>

c'est-à-dire que $G_{k^s} \simeq (\mathbb{G}_m)^n$ pour un n.

Décrivons les tores de dim 1 sur $k = \mathbb{R}$. Alors $\Gamma = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$
$= \mathbb{Z}/2\mathbb{Z}$

En dim 1 le groupe abélien M est $\mathbb{Z}$

On a $\mathrm{Aut}_{gr}(\mathbb{Z}) = \{\pm 1\} = \mathbb{Z}/2\mathbb{Z}$ et il y a deux actions

non isomorphes de Γ : la triviale et id : $\Gamma = \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z})$.

La triviale donnera le $\mathbb{R}$-groupe $\mathbb{G}_{m,\mathbb{R}}$; regardons l'autre.

On a $\mathbb{C}[\mathbb{Z}] = \mathbb{C}[z, z^{-1}]$ qui est muni de l'action de $\Gamma = \langle \sigma \rangle$

conj. complexe

- action naturelle sur $\mathbb{C}$ (conj. compl.)
- action par $\sigma(z) = z^{-1}$ sur la variable, correspondant à l'action non triviale sur $\mathbb{Z}$.

L'anneau d'invariants $\mathbb{C}[z, z^{-1}]^{\Gamma}$ est une $\mathbb{R}$-algèbre

engendrée par $x = \frac{z + z^{-1}}{2}$ et $y = \frac{iz - iz^{-1}}{2}$ avec une relation :

on a $z = x - iy$ et $z^{-1} = x + iy$ donc

$$1 = zz^{-1} = (x - iy)(x + iy) = x^2 + y^2$$

On obtient $G = \mathrm{Spec}\left(\mathbb{C}[\mathbb{Z}]^{\Gamma}\right) = \mathrm{Spec}\, \dfrac{\mathbb{R}[x,y]}{x^2 + y^2 - 1} = S^1$ le cercle !

On vérifie que la loi de groupe est celle du cercle...

On termine par un petit résultat qui illustre comment on démontre en pratique un résultat sur les groupes de type mult. en se ramenant au cas diagonalisable :

__Cor__ Soit G un k-gr de type multiplicatif. Alors G possède un unique tore maximal ie ss-gr lisse connexe maximal.

__Dém.__ • Si $G = D(M)$ diagonalisable, un sous-groupe est un $H = D(N)$ avec $M \twoheadrightarrow N$ quotient.

De plus H est lisse ssi N est sans p-torsion, $p = car(k)$

connexe ssi N est sans n-torsion, $p \nmid n$

Donc on veut H sans torsion. Or il y a un plus grand tel H, c'est $M/Tors(M)$.

• Si G quelconque, alors d'après le cas précédent dans $G_{k^s} = D_{k^s}(M)$ il y a un unique $H \subset G_{k^s}$ lisse connexe maximal

Celui-ci est donc stable par $\Gamma = Gal(k^s/k)$ i.e. l'action de Γ sur G_{k^s} induit une action sur $H = spec\, k[P]$

P : un module

et $H_0 = spec\, k[P]^\Gamma$ est le sous-groupe recherché $\boxtimes$