Introduction aux groupes arithmétiques

GdT Topologie de $\mathcal{A}_g$

Arthur Garnier

Laboratoire Amiénois de Mathématique Fondamentale et Appliquée
Université de Picardie Jules Verne

8 juin 2021

Définitions

Groupe algébrique = variété algébrique + structure de groupe.

Définition

k un corps, une k-variété (k-schéma) $\mathbf{G}$ est un *groupe algébrique* s'il existe des morphismes $\mu : \mathbf{G} \times_k \mathbf{G} \longrightarrow \mathbf{G}$, $\iota : \mathbf{G} \longrightarrow \mathbf{G}$ et $e : \mathrm{Spec}(k) \longrightarrow \mathbf{G}$ vérifiant les axiomes usuels de groupes.

$\mathbf{G}$ est lisse et donné avec un morphisme $\mathbf{G} \to \mathrm{Spec}(k)$ et le groupe des *k-points* de $\mathbf{G}$ est

$$\mathbf{G}(k) := \{\sigma : \mathrm{Spec}(k) \to \mathbf{G} \text{ section de } \mathbf{G} \to \mathrm{Spec}(k)\}.$$

Si k est algébriquement clos, une variété $\mathbf{G}$ est un gp alg ssi les k-points $\mathbf{G}(k)$ forment un groupe. On "identifie" alors $\mathbf{G}$ et $\mathbf{G}(k)$.

On se concentre sur les groupes algébriques affines $\mathbf{G} = \mathrm{Spec}(A)$.
Remarque : $\mathrm{Spec}(A)$ est un gp alg ssi A *algèbre de Hopf*.

Premiers exemples

Exemple

- Groupe additif : $\mathbb{G}_a := (k, +) \simeq \mathrm{Spec}(k[X])$.
- Groupe multiplicatif : $\mathbb{G}_m := (k^\times, \times) \simeq \mathrm{Spec}(k[X, X^{-1}])$.
- Groupe linéaire :

$$GL_n(k) = \{(g_{i,j}) \in \mathcal{M}_n(k) \ ; \ \det(g_{i,j}) \neq 0\}$$

$$\simeq \{(x_{i,j}, z) \ ; \ \det(x_{i,j})z = 1\} = \mathrm{Spec}(k[X_{i,j}, Z]/(\det(X_{i,j})Z - 1)).$$

- Groupe spécial :

$$SL_n(k) = \mathrm{Spec}(k[X_{i,j}]/(\det(X_{i,j}) - 1)).$$

Quelques propriétés

- Topologie de $\mathbf{G} \times_k \mathbf{G} \neq$ topologie produit : algébrique $\not\Rightarrow$ topologique.
- $\mathbf{G}$ affine ssi linéaire, i.e. $\mathbf{G} \hookrightarrow GL_n(k)$. Dans ce cas, on peut écrire

$$\mathbf{G} = \mathrm{Spec}\left(\frac{k[X_{i,j}, Z]}{(\det(X_{i,j})Z - 1) + \mathfrak{a}}\right),$$

avec $\mathfrak{a} = (P_a(X_{i,j}),\ a \in A)$ idéal (A fini) et

$$\mathbf{G}(k) = \{g = (g_{i,j}) \in GL_n(k)\ ;\ P_a(g_{i,j}) = 0,\ \forall a \in A\}.$$

À partir de maintenant, on suppose $k = \mathbb{C}$.

Rationalité et corps de définition

Groupe défini sur un sous corps $k' \subset k$: $\mathbf{G}/k$ est *défini sur* k' s'il existe $\mathbf{G}'/k'$ tq $\mathbf{G} = \mathrm{Spec}(k) \times_{k'} \mathbf{G}'$ i.e.

$$\begin{array}{ccc} \mathbf{G} & \xrightarrow{\exists} & \exists \mathbf{G}' \\ \downarrow & \lrcorner & \downarrow \\ \mathrm{Spec}(k) & \xrightarrow{\text{can.}} & \mathrm{Spec}(k') \end{array}$$

Ça veut dire que les équations qui définissent $\mathbf{G}$ sont à coefficients dans k'.

Exemple

- $GL_n(\mathbb{C})$, $SL_n(\mathbb{C})$, $\mathbb{G}_a^{\mathbb{C}}$, $\mathbb{G}_m^{\mathbb{C}}$ sont définis sur $\mathbb{Q}$.
- $\left\{ \begin{pmatrix} 1 & x & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \pi x \\ 0 & 0 & 0 & 1 \end{pmatrix} \in GL_4(\mathbb{C}) \right\} \simeq \{(x, y) \in \mathbb{A}^2_{\mathbb{C}} \ ; \ y = \pi x\}$ n'est pas défini sur $\mathbb{Q}$.

Formes quadratiques et groupes orthogonaux

$q : \mathbb{C}^n \to \mathbb{C}$ forme bilinéaire non-dég. de matrice A. On définit

$$O(q) := \{g \in GL_n(\mathbb{C}) \ ; \ q(gv) = q(v), \ \forall v \in \mathbb{C}^n\}$$

$$= \{g \in GL_n(\mathbb{C}) \ ; \ {}^t gAg = A\}.$$

C'est un grp alg (défini sur $\mathbb{Q}$ si $A \in \mathcal{M}_n(\mathbb{Q})$), ainsi que $SO(q) := O(q) \cap SL_n(\mathbb{C})$.

Remarque : si $\omega := dx_1 \wedge \cdots \wedge dx_n \in \Omega^n(\mathbb{C}^n)$, alors $SL_n(\mathbb{C}) = \{g \in GL_n(\mathbb{C}) \ ; \ g^*\omega = \omega\}$.

Comme $O(q)$, SL_n se voit comme un groupe linéaire préservant une structure supplémentaire sur $\mathbb{C}^n$ (les formes volume).

Formes quadratiques et groupes orthogonaux

Exemple

- $\omega(X,Y) = x_1y_{2n} + x_2y_{2n-1} + \cdots + x_ny_{n+1} - x_{n+1}y_n - \cdots - x_{2n}y_1$ symplectique, alors

$$Sp_n(\mathbb{C}) := \{g \in SL_{2n}(\mathbb{C}) \ ; \ \omega(gX, gY) = \omega(X,Y)\}$$

$$= \{g \in SL_{2n}(\mathbb{C}) \ ; \ {}^tgJg = J\} \text{ où } J = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}.$$

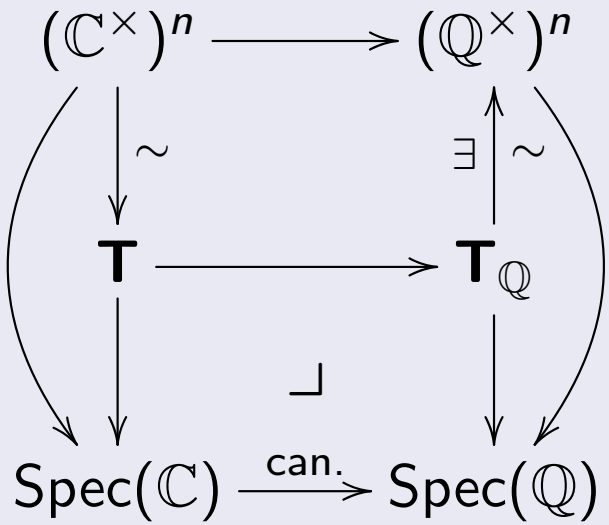
- $\langle X, Y\rangle = x_1y_n + x_2y_{n-1} + \ldots + x_ny_1$ symétrique, alors

$$SO_n(\mathbb{C}) = \{g \in SL_n(\mathbb{C}) \ ; \ {}^tgAg = A\} \text{ où } A = \begin{pmatrix} (0) & & 1 \\ & \iddots & \\ 1 & & (0) \end{pmatrix}.$$

Tores et tores déployés (ou scindés)

Définition

- Un *tore* est un gp alg $\mathbf{T}$ connexe isomorphe à $(\mathbb{G}_m^{\mathbb{C}})^n = (\mathbb{C}^\times)^n$ pour un certain $n = \dim \mathbb{T}$ (on fixe aussi l'isomorphisme).
- Si l'iso $\mathbb{T} \xrightarrow{\sim} (\mathbb{C}^\times)^n$ est défini sur $\mathbb{Q}$, $\mathbf{T}$ est dit *déployé sur* $\mathbb{Q}$. Ceci signifie



- On peut faire la même chose sur tout corps $\mathbb{Q} \subset K \subset \mathbb{C}$.

Tores et tores déployés (ou scindés)

Exemple

- $\mathbf{T}_1 := SO_2(\mathbb{C}) = \{g \in SL_2(\mathbb{C}) \ ; \ {}^t g \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} g = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}\}$. On a un iso $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mapsto a$ de $\mathbf{T}_1$ dans $\mathbb{C}^\times$, défini sur $\mathbb{Q}$. Donc $\mathbf{T}_1$ est déployé.
- $\mathbf{T}_2 := \{g \in SL_2(\mathbb{C}) \ ; \ {}^t g g = I_2\}$. C'est un tore défini sur $\mathbb{Q}$ mais non déployé sur $\mathbb{R}$. En effet, $\mathbf{T}_2(\mathbb{R}) = SO_2(\mathbb{R})$ est compact. C'est bien un tore car $\mathbf{T}_1 = SO(2xy)$ et $\mathbf{T}_2 = SO(x^2 + y^2)$, et les 2 formes sont équivalentes sur $\mathbb{C}$.
- $\mathbf{T}_3 := SO(x^2 - 2y^2) = \{g \in SL_2 \ ; \ {}^t g \begin{pmatrix} 1 & \\ & -2 \end{pmatrix} g = \begin{pmatrix} 1 & \\ & -2 \end{pmatrix}\}$. On a $x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$, donc $\mathbf{T}_3$ est déployé sur $\mathbb{R}$, pas sur $\mathbb{Q}$.

Tores et tores déployés (ou scindés)

Théorème de Grothendieck

G groupe affine connexe.

- Il existe un tore maximal $\mathbf{T} < \mathbf{G}$ tq $\mathbf{T}_{\overline{k}} < \mathbf{G}_{\overline{k}}$ est maximal.
- Pour tout k-tore $\mathbf{T} < \mathbf{G}$ et toute extension K/k, le tore $\mathbf{T}_K < \mathbf{G}_K$ est maximal.
- Il existe K/k finie tq $\mathbf{G}_K$ admet un K-tore déployé.

Ceci signifie qu'on peut "ramener" l'étude des tores et systèmes de racines au cas des corps algébriquement clos.

Groupes unipotents, résolubles, radicaux

Définition

- Un gp alg $\mathbf{G} \hookrightarrow GL_n(\mathbb{C})$ est *unipotent* si $\forall g \in \mathbf{G}(\mathbb{C}) \subset GL_n(\mathbb{C})$, $g - I_n$ est nilpotent. Par Jordan, c'est indépendant du plongement.
- $\mathbf{G}$ est résoluble s'il l'est comme groupe abstrait.
- Le *radical* (*unipotent*) de $\mathbf{G}$ est le sous-groupe $R(\mathbf{G})$ (resp. $R_u(\mathbf{G})$) résoluble (unipotent) connexe normal maximal de $\mathbf{G}$.
- $\mathbf{G}$ est *semi-simple* (*réductif*) si $R(\mathbf{G}) = 1$ ($R_u(\mathbf{G}) = 1$).

Exemple

- $\mathbf{G}_a = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right),\ a \in \mathbb{C}\}$ est unipotent.
- $\{$matrices triang. sup.$\} \subset GL_n(\mathbb{C})$ est résoluble.
- $\mathbf{G}/R(\mathbf{G})$ est semi-simple et $\mathbf{G}/R_u(\mathbf{G})$ est réductif.

Rang et $\mathbb{Q}$-rang

Soit $\mathbf{G}/\mathbb{C}$ réductif connexe. Tous les tores max. de $\mathbf{G}$ sont conjugués et leur dimension commune est le *rang* $\mathrm{rg}_{\mathbb{C}}(\mathbf{G})$ de $\mathbf{G}$.

Si $\mathbf{G}$ est défini sur $\mathbb{Q}$, tous les $\mathbb{Q}$-tores sont $\mathbf{G}(\mathbb{Q})$-conjugués et on définit de même $\mathrm{rg}_{\mathbb{Q}}(\mathbf{G})$. $\mathbf{G}$ est dit déployé si $\mathrm{rg}_{\mathbb{Q}}(\mathbf{G}) = \mathrm{rg}_{\mathbb{C}}(\mathbf{G})$.

Exemple

- Il n'y a pas égalité en général (cf $\mathbf{T}_{1,2,3}$ ci-dessus).
- $\mathbf{G} = SL_n(\mathbb{C})$ est déployé sur $\mathbb{Q}$ et $\mathrm{rg}(\mathbf{G}) = n - 1$.

Un premier lien entre gp algs et arithmétique :

Proposition

Soit q forme quadratique rationnelle non-dég. sur un $\mathbb{Q}$-ev V. Alors

$$\mathrm{rg}_{\mathbb{Q}}(O(q)) > 0 \iff \exists v \in V \setminus \{0\} \ ; \ q(v) = 0.$$

Preuve de la proposition

Si $1 \neq \mathbf{T} < O(q)$ tore $\mathbb{Q}$-déployé, on diagonalise

$$V = \oplus_\lambda V_\lambda \text{ où } V_\lambda = \{v \in V \ ; \ \forall t \in \mathbf{T}, \ t \cdot v = \lambda(t)v\},$$

où $\lambda : \mathbf{T} \to \mathbb{C}^\times$ caractère provenant de $\lambda_\mathbb{Q} : \mathbf{T}_\mathbb{Q} \to \mathbb{Q}^\times$. Comme $\mathbf{T} \circlearrowright \mathbb{C}^n$ non-triviale, $\exists \lambda_0 \neq 1$ dans la décompo. et soit $v \in V_{\lambda_0} \setminus \{0\}$. Pour $t \in \mathbf{T}$ tq $\lambda_0(t^2) \neq 1$ on a

$$q(v) = q(t \cdot v) = q(\lambda_0(t)v) = \lambda_0(t^2)q(v) \implies q(v) = 0.$$

Si $0 \neq v_1 \in V$ isotrope, on complète en plan hyperbolique $\langle v_1, v_2 \rangle$ et soit $v_3, \ldots, v_n$ base de $\langle v_1, v_2 \rangle^\perp$. Si $(x_1, \ldots, x_n)$ coordonnées pour cette base, on écrit $q(x_1, \ldots, x_n) = x_1x_2 + q'(x_3, \ldots, x_n)$ et $\mathbf{T} := \mathbb{C}^\times$ agit sur $\mathbb{C}^n$ par

$$x_1 \mapsto tx_1, \ x_2 \mapsto t^{-1}x_2, \ x_i \mapsto x_i \ (i \geq 3),$$

en préservant q et donc $\mathbf{T} < O(q)$. □

Sous-groupes de Borel, paraboliques

Définition

$\mathbf{G}/\mathbb{C}$ connexe.

- Un sous-groupe fermé $\mathbf{B} < \mathbf{G}$ résoluble connexe maximal est dit *de Borel*.
- Un sous-groupe fermée $\mathbf{P} < \mathbf{G}$ est *parabolique* s'il contient un Borel (ssi $\mathbf{G}/\mathbf{P}$ variété projective, ssi $\mathbf{G}(\mathbb{C})/\mathbf{P}(\mathbb{C})$ compacte.
- Si $\mathbf{G}$ défini sur $\mathbb{Q}$ et si $\mathbf{P} < \mathbf{G}$ parabolique défini sur $\mathbb{Q}$, on dit que $\mathbf{P}$ est *rationnel*.

Faits : Les paraboliques rationnels minimaux sont $\mathbf{G}(\mathbb{Q})$-conjugués. Tout para. rat. min. fixé $\mathbf{P}$ est inclus dans un nb. fini de para. rat. (dits *standards* et décrits par les *racines* de $(\mathbf{G}, \mathbf{T})$, avec $\mathbf{T} < \mathbf{P}$. Les para. rat. min. sont des Borel rat. si $\mathbf{G}$ en admet au-moins un.

Exemple de GL_n

$\mathbf{G} := GL_n(\mathbb{C})$ est réductif connexe (non semi-simple car $Z(\mathbf{G}) = \mathbb{C}^\times I_n$ donc $1 \neq Z(\mathbf{G}) \leq R(\mathbf{G})$). Aussi, $\mathbf{G}' = SL_n(\mathbb{C})$ et $\mathbf{G} = R(\mathbf{G}) \cdot \mathbf{G}'$ (fait général).

Le tore $\mathbf{T} = \{\mathrm{diag}(t_1, \ldots, t_n),\ t_i \in \mathbb{C}^\times\}$ est maximal $\mathbb{Q}$-déployé et $\mathrm{rg}_{\mathbb{Q}}(\mathbf{G}) = n = \mathrm{rg}_{\mathbb{Q}}(\mathbf{G})$. Le sous-groupe $\mathbf{B} := \left\{ \begin{pmatrix} t_1 & & (*) \\ & \ddots & \\ (0) & & t_n \end{pmatrix} \right\}$ est un parabolique rationnel minimal et un Borel. Les para. rat. standards sont les groupes de matrices triang. sup. par blocs.

Dans ce cas, la *variété de drapeaux* $\mathbf{G}/\mathbf{B}$ s'identifie à l'ensemble des drapeaux i.e.

$$(\mathbf{G}/\mathbf{B})(\mathbb{C}) \approx \{(V_0 \leq V_1 \leq \ldots \leq V_n)\ ;\ V_i \leq \mathbb{C}^n \ \&\ \dim V_i = i\}.$$

Objet important en théorie de Lie, exemple : les $\mathbf{G}$-modules simples sont les sections globales de fibrés en droites sur $\mathbf{G}/\mathbf{B}$ (Borel-Weil).

Commensurabilité et notion de groupe arithmétique

Slogan : Groupes arithmétiques $=$ $\mathbb{Z}$-points des groupes sur $\mathbb{Q}$.

Pour $\mathbf{G}/\mathbb{Q}$ plongé $\mathbf{G} \leq GL_n(\mathbb{C})$, on pourrait définir un groupe arithmétique comme étant de la forme $\Gamma = GL_n(\mathbb{Z}) \cap \mathbf{G}(\mathbb{Q})$.

Problème : Non-invariant par $\mathbb{Q}$-isomorphisme. Du coup, on remplace Γ ci-dessus par un sous-groupe lui étant *commensurable*.

Définition

- Deux sous-groupes $H_1, H_2 \leq G$ sont *commensurables* (noté $H_1 \sim H_2$) si $H_1 \cap H_2$ est d'indice fini dans H_1 et H_2.
- $\mathbf{G}/\mathbb{C}$ groupe défini sur $\mathbb{Q}$ plongé dans $GL_n(\mathbb{C})$. Un sous-groupe $\Gamma \leq \mathbf{G}(\mathbb{Q})$ est *arithmétique* si $\Gamma \sim \mathbf{G}(\mathbb{Z})$.

Lemme

Si $\varphi : \mathbf{G}/\mathbb{Q} \xrightarrow{\sim} \mathbf{G}'/\mathbb{Q}$ *alors* $\varphi(\mathbf{G}(\mathbb{Z})) \sim \mathbf{G}'(\mathbb{Z})$.

Preuve du lemme

Il faut mq

$$[\varphi(\mathbf{G}(\mathbb{Z})) : \varphi(\mathbf{G}(\mathbb{Z})) \cap \mathbf{G}'(\mathbb{Z})] < \infty \ \& \ [\varphi^{-1}(\mathbf{G}'(\mathbb{Z})) : \varphi^{-1}(\mathbf{G}'(\mathbb{Z})) \cap \mathbf{G}(\mathbb{Z})] < \infty.$$

Quitte à $\varphi \leftrightarrow \varphi^{-1}$, il suffit de prouver la première. Il suffit de trouver $\Gamma' \leq \mathbf{G}(\mathbb{Z})$ d'indice fini tq $\varphi(\Gamma') \leq \mathbf{G}'(\mathbb{Z})$. En effet, on aura alors

$$[\varphi(\mathbf{G}(\mathbb{Z})) : \varphi(\mathbf{G}(\mathbb{Z})) \cap \mathbf{G}'(\mathbb{Z})] \cdot [\varphi(\mathbf{G}(\mathbb{Z})) \cap \mathbf{G}'(\mathbb{Z}) : \varphi(\Gamma')] = [\varphi(\mathbf{G}(\mathbb{Z})) : \varphi(\Gamma')] \leq [\mathbf{G}(\mathbb{Z}) : \Gamma'] < \infty.$$

Voyant $\mathbf{G} \subset \mathcal{M}_m(\mathbb{C})$ et $\mathbf{G}' \subset \mathcal{M}_n(\mathbb{C})$, on peut supposer $\varphi((x_{i,j})) = (\varphi_{k,l}(x_{i,j}))_{k,l}$ avec $\varphi_{k,l} \in \mathbb{Q}[X_{i,j}]$. On pose $y_{i,j} := x_{i,j} - \delta_{i,j}$ et $\psi_{k,l}(y_{i,j}) := \varphi_{k,l}(x_{i,j}) - \delta_{k,l}$. On a $\psi_{k,l}(0) = 0$. Soient $d \in \mathbb{Z}$ tq $d\psi_{k,l} \in \mathbb{Z}[Y_{i,j}]$ et

$$\Gamma' := \{g \in \mathbf{G}(\mathbb{Z}) \, ; \, g \equiv id[d]\} = \ker(\mathbf{G}(\mathbb{Z}) \hookrightarrow GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/d\mathbb{Z})).$$

Si $g \in \Gamma'$, alors $d|(g - id)$ donc $\psi(g - id) \in \mathcal{M}_n(\mathbb{Z})$ et donc $\varphi(g) = \psi(g - id) + id \in \mathbf{G}'(\mathbb{Z})$, d'où $\varphi(\Gamma') \leq \mathbf{G}'(\mathbb{Z})$. □

Cas des corps de nombres

Corollaire

- *Si* $\varphi : \mathbf{G}/\mathbb{Q} \xrightarrow{\sim} \mathbf{G}'/\mathbb{Q}$ *et* $\Gamma \leq \mathbf{G}(\mathbb{Q})$. *Alors* Γ *arithmétique ssi* $\varphi(\Gamma)$ *arithmétique.*
- *Si* $\Gamma \leq \mathbf{G}(\mathbb{Q})$ *arithmétique et* $g \in \mathbf{G}(\mathbb{Q})$, *alors* $g\Gamma g^{-1} \leq \mathbf{G}(\mathbb{Q})$ *aussi.*

Généralisation ?

Soient $\mathbb{F}$ un corps de nombres (une extension finie de $\mathbb{Q}$), $\mathcal{O}_{\mathbb{F}}$ son anneau d'entiers et $\mathbf{G}$ un groupe alg. linéaire défini sur $\mathbb{F}$.

Définition

Un sous-groupe $\Gamma \leq \mathbf{G}(\mathbb{F})$ est *arithmétique* si $\Gamma \sim \mathbf{G}(\mathcal{O}_{\mathbb{F}})$.

arithmétique/$\mathbb{F} \Rightarrow$ arithmétique/$\mathbb{Q}$, mais peut être utile d'utiliser des corps de nombres pour définir les groupes arithmétiques.

Foncteur de restriction des scalaires

On construit un foncteur

$$\mathrm{Res}_{\mathbb{F}/\mathbb{Q}} : \mathbf{Grp}_{\mathbb{F}} \longrightarrow \mathbf{Grp}_{\mathbb{Q}}$$

tel que $(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}\mathbf{G})(\mathbb{Q}) = \mathbf{G}(\mathbb{F})$ et $(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}\mathbf{G})(\mathbb{Z}) \sim \mathbf{G}(\mathcal{O}_{\mathbb{F}})$.

Pour $x \in \mathbb{F}$, on regarde $\mu_x := (y \mapsto xy) \in \mathrm{End}_{\mathbb{Q}}(\mathbb{F})$. Choisissons une base $v_1, \dots, v_d$ de $\mathbb{F}/\mathbb{Q}$ et notons $\rho(x) := \mathrm{Mat}_{(v_i)}(\mu_x)$, d'où une représentation fidèle

$$\rho : \mathbb{F} \hookrightarrow \mathcal{M}_d(\mathbb{Q}).$$

Soient $f_1, \dots, f_r$ formes $\mathbb{Q}$-linéaires sur $\mathbb{F}$ telles que

$$\rho(\mathbb{F}) = \{(y^{\alpha,\beta})_{\alpha,\beta} \in \mathcal{M}_d(\mathbb{Q}) \ ; \ f_1(y^{\alpha,\beta}) = \cdots = f_r(y^{\alpha,\beta}) = 0\}.$$

Foncteur de restriction des scalaires

Supposons

$$\mathbf{G} = \{g \in GL_n(\mathbb{C}) \ ; \ P_i(g) = 0, \ \forall i \in I\} \text{ avec } I \text{ fini et } P_i \in \mathbb{F}[X_{i,j}].$$

Écrivons

$$P_i(g) = \sum_{\gamma_{i,j}} a_{\gamma_{1,1},\dots,\gamma_{n,n}} g_{1,1}^{\gamma_{1,1}} \cdots g_{n,n}^{\gamma_{n,n}} \text{ avec } a_{\gamma_{i,j}} \in \mathbb{F}.$$

On définit $\widetilde{P}_i(y)$ à coefficients dans $\mathcal{M}_d(\mathbb{Q})$ par

$$\widetilde{P}_i(y) := \sum_{\gamma_{i,j}} \rho(a_{\gamma_{1,1}\dots,\gamma_{n,n}})((y_{1,1}^{\alpha,\beta})_{\alpha,\beta})^{\gamma_{1,1}} \cdots ((y_{n,n}^{\alpha,\beta})_{\alpha,\beta})^{\gamma_{n,n}} \in \mathcal{M}_d(\mathbb{Q}[y_{i,j}^{\alpha,\beta}]).$$

Voyant $GL_{nd}(\mathbb{C}) \subset \mathcal{M}_{nd}(\mathbb{C}) \simeq \mathcal{M}_n(\mathcal{M}_d(\mathbb{C}))$, on pose

$$\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(\mathbf{G}) := \left\{ (y_{1,1}^{\alpha,\beta})_{\alpha,\beta}, \dots, (y_{n,n}^{\alpha,\beta})_{\alpha,\beta} \;\middle|\; \begin{array}{l} \forall i,j,k, \ f_k(y_{i,j}^{\alpha,\beta}) = 0 \\ \forall i \in I, \ \widetilde{P}_i(y) = 0 \end{array} \right\}.$$

À $\mathbb{Q}$-iso près, $\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(\mathbf{G})$ ne dépend pas de la base (v_i) choisie.

Interprétation de $\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(\mathbf{G})$ via les plongements $\mathbb{F} \hookrightarrow \overline{\mathbb{Q}}$

Les équations définissant $\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(\mathbf{G})$ permettent de le voir comme $\mathbf{G}(\mathbb{F} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})$. Si $\sigma_1, \dots, \sigma_d$ sont les $\mathbb{Q}$-plongements $\mathbb{F} \hookrightarrow \overline{\mathbb{Q}}$, alors on a un plongement $\mathbb{F} \hookrightarrow \overline{\mathbb{Q}}^d$, $x \mapsto (\sigma_1(x), \dots, \sigma_d(x))$ et $\mathbb{F} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}^d$. D'où un $\overline{\mathbb{Q}}$-iso

$$\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(\mathbf{G}) \simeq \mathbf{G}^{\sigma_1} \times \cdots \times \mathbf{G}^{\sigma_d},$$

où, si $\mathbf{G}_{\mathbb{F}} = \mathrm{Spec}(\mathbb{F}[X_{i,j}, Z]/\mathfrak{a})$, alors $\mathbf{G}^{\sigma_i} := \mathrm{Spec}(\mathbb{C}[X_{i,j}, Z]/\mathfrak{a}^{\sigma_i})$ avec $\mathfrak{a}^{\sigma_i} = \{\sigma_i(a),\ a \in \mathfrak{a}\}$. En particulier, si $\mu_1, \dots, \mu_s : \mathbb{F} \hookrightarrow \mathbb{R}$ et $\mu_{s+1}, \overline{\mu_{s+1}}, \dots, \mu_{s+t}, \overline{\mu_{s+t}} : \mathbb{F} \hookrightarrow \mathbb{C}$, alors

$$(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}\mathbf{G})(\mathbb{R}) \simeq \prod_{i=1}^{s+t} \mathbf{G}(\mathbb{F}^{\mu_i}).$$

Groupes arithmétiques comme sous-groupes discrets de groupes de Lie

$\mathbf{G}/\mathbb{C}$ connexe défini sur $\mathbb{Q}$, alors $\mathbf{G}(\mathbb{R})$ est un groupe de Lie. Si $\Gamma \leq \mathbf{G}(\mathbb{Q})$ arithmétique, alors Γ sous-groupe discret de $\mathbf{G}(\mathbb{R})$.

Si $\mathbf{G}$ défini sur un corps de nombres $\mathbb{F}$ et $\Gamma \leq \mathbf{G}(\mathbb{F})$, alors Γ est discret dans $(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}\mathbf{G})(\mathbb{R}) = \prod_{i=1}^{s+t} \mathbf{G}(\mathbb{F}^{\mu_i})$.

Si $s + t > 1$ alors $\mathbf{G}(\mathcal{O}_{\mathbb{F}})$ n'est pas discret dans $\mathbf{G}(\mathbb{F}^{\sigma_i})$.

Exemple

$\mathbb{F} = \mathbb{Q}(\sqrt{5})$, alors $(x, t) = (2, 0)$ et l'image de $GL_2(\mathcal{O}_{\mathbb{F}}) = GL_2(\mathbb{Z}[\frac{1}{2}(1+\sqrt{5})])$ dans $GL_2(\mathbb{R})$ n'est pas discrète (car $\mathbb{Z}[\frac{1}{2}(1+\sqrt{5})] \subset \mathbb{R}$ est dense).

Groupes arithmétiques comme sous-groupes discrets de groupes de Lie

Exemple

- $\mathbb{G}_a = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right),\ a \in \mathbb{C}\}$ est défini sur $\mathbb{F}$, pour toute $\mathbb{F}/\mathbb{Q}$ et $\mathbb{G}_a(\mathcal{O}_\mathbb{F}) = \mathcal{O}_\mathbb{F}$. $\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(\mathbb{G}_a)$ est isomorphe au commutant de $\varrho(\mathbb{F})$ dans $\mathcal{M}_d(\mathbb{C})$ (exercice !) et l'image de $\mathcal{O}_\mathbb{F}$ dans

$$\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}\mathbb{G}_a(\mathbb{R}) = \prod_{i=1}^{s+t} \mathbb{G}_a(\mathbb{F}^{\mu_i}) = \mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^{s+2t}$$

est un réseau.

- $\mathbb{G}_m = GL_1$ est défini sur $\mathbb{Q}$ et si $N(x) := \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{Q})} \sigma(x)$ est la norme de $\mathbb{F}/\mathbb{Q}$, alors on peut regarder $\mathcal{N} := \{g \in \mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(GL_1)\ ;\ N(g) = 1\} \leq \mathbb{G}_m(\mathbb{F})$ et alors $\mathcal{O}_\mathbb{F}^\times \leq \mathcal{N}$ est discret.

Reformulation en termes de réseaux

On a fixé une structure entière sur un $\mathbb{Q}$-ev en fixant une base.
Autre point de vue : réseau compatible à la structure rationnelle.

Soient V un $\mathbb{Q}$-ev et $L \subset V$ un réseau. On définit

$$GL(V, L) := \{g \in GL(V) \ ; \ gL = L\}.$$

Si $\mathbf{G} \hookrightarrow GL(V \otimes_{\mathbb{Q}} \mathbb{C})$ défini sur $\mathbb{Q}$, le *groupe des L-unités* de $\mathbf{G}$ est

$$\mathbf{G}(L) := \mathbf{G}(\mathbb{Q}) \cap GL(V, L).$$

Proposition

$\Gamma \leq \mathbf{G}(\mathbb{Q})$ arithmétique ssi $\Gamma \sim \mathbf{G}(L)$ pour un réseau L.

De même si V est un $\mathbb{F}$-ev ($\mathbb{F}/\mathbb{Q}$ finie) et $L \subset V$ un réseau (i.e. un sous-$\mathcal{O}_{\mathbb{F}}$-module de type fini de V), on définit $GL(V, L)$, $\mathbf{G}(L)$ et on a la proposition ci-dessus.

Paires symétriques

G connexe défini sur $\mathbb{Q}$ et $G := \mathbf{G}(\mathbb{R})$ groupe de Lie. Si $K < G$ compact et $\sigma : G \to G$ involution tq $G^{\sigma,0} \subset K \subset G^{\sigma}$, on dit que (G, K) est une *paire symétrique*. Dans ce cas, $X := G/K$ est un espace symétrique.

Remarque : si X symétrique, $G = \mathrm{Is}(X)^0$ et $K = \mathrm{Stab}_G(x_0)$, on pose $\sigma(g) := s_{x_0} g s_{x_0}$. Alors $X \simeq G/K$ et (G, K) est une paire symétrique.

Si G est semi-simple non-compact, alors il existe une unique involution σ (à aut. int. près) tq $G^{\sigma} < G$ soit compact maximal. Il y a donc un unique espace symétrique de type non-compact associé à G.

Quelques résultats sans preuves

Théorème

$\mathbf{G}$ connexe semi-simple défini sur $\mathbb{Q}$ et $\Gamma \leq \mathbf{G}(\mathbb{Q})$ arithmétique.

- $\Gamma \leq \mathbf{G}(\mathbb{Z}) \Rightarrow \Gamma$ a un sous-groupe d'indice fini sans torsion.
- LASSE
  - L'espace localement symétrique $\Gamma\backslash G$ est compact.
  - $\mathbf{G}(\mathbb{Q})$ ne contient pas d'unipotent non-trivial.
  - $\mathrm{rg}_{\mathbb{Q}}(\mathbf{G}) = 0$.

Si $\Gamma < G$ discret, si $\Gamma \curvearrowright G/K = X$ est propre et si $\mathrm{Tors}(\Gamma) = 1$, alors $\Gamma \curvearrowright X$ est libre et $\Gamma\backslash X$ espace loc. symétrique.

Théorème

$\mathbf{G}$ connexe réductif défini sur $\mathbb{Q}$ et $\Gamma \leq \mathbf{G}(\mathbb{Q})$ arithmétique. Alors $\Gamma\backslash\mathbf{G}(\mathbb{R})$ compact ssi $\mathbf{G}$ n'a aucun caractère non-trivial sur $\mathbb{Q}$ et si $\mathbf{G}(\mathbb{Q})$ n'a pas d'unipotent non-trivial.

Rappels sur les algèbres de quaternions

Soient $a, b \in \mathbb{Q}^\times$. $\mathcal{H}(a,b)$ est la $\mathbb{Q}$-algèbre de base $1, i, j, k$ tels que

$$i^2 = a,\ j^2 = b,\ ij = -ji = k.$$

Exemple : quaternions usuels avec $a = b = -1$. On a une représentation fidèle

$$\begin{array}{rccc} \rho & : & \mathcal{H}(a,b) & \hookrightarrow & \mathcal{M}_2(\mathbb{Q}(\sqrt{a})) \\ & & x+yi+zj+tk & \longmapsto & \begin{pmatrix} x+y\sqrt{a} & z+t\sqrt{a} \\ b(z-t\sqrt{a}) & x-y\sqrt{a} \end{pmatrix} \end{array}$$

et on a aussi $\mathcal{H}(a,b) \hookrightarrow \mathcal{M}_4(\mathbb{Q})$. Remarque : si $a \in (\mathbb{Q}^\times)^2$, alors $\mathcal{H}(a,b) \simeq \mathcal{M}_2(\mathbb{Q})$. Pour $q = x + yi + zj + tk$, on a la conjugaison $\iota : \mathcal{H}(a,b) \to \mathcal{H}(a,b)$, $\iota(q) = x - yi - zj - tk$, la trace $\mathrm{Tr}(q) := q + \iota q = 2x$ et la norme $\mathrm{Nr}(q) := q \cdot \iota q = x^2 - ay^2 - bz^2 + abt^2$.

Rappels sur les algèbres de quaternions

Proposition

- *$\mathcal{H}(a,b)$ est iso à $\mathcal{M}_2(\mathbb{Q})$ ou est une algèbre à division.*
- *$\mathcal{H}(a,b)$ à division ssi $\mathrm{Nr}(q) \neq 0$ pour $q \neq 0$.*
- *p premier, a entier non-carré modulo p. Alors $\mathcal{H}(a,p)$ est à division.*

Preuve : Sinon, $\exists q = x + yi + zj + tk \neq 0$ tq $\mathrm{Nr}(q) = 0$. On peut supposer $x, y, z, t \in \mathbb{Z}$ sans facteur commun. Alors on a $x^2 = ay^2[p]$ et si $y \neq 0[p]$, alors $a = \left(\frac{x}{y}\right)^2 [p]$, contradiction. Donc $p|y$ et $p|x$. Comme $\mathrm{Nr}(x) = 0$, on a aussi $z^2 = at^2[p]$ et on conclut de même $p|z$ et $p|t$, contradiction. □

Groupes fuchsiens arithmétiques

On suppose $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$ et $\mathcal{H}(a,b)$ à division. On définit

$$\mathcal{O} := \{x + yi + zj + tk \in \mathcal{H}(a,b) \ ; \ x,y,z,t \in \mathbb{Z}\},$$

$$\Gamma := \{q \in \mathcal{O} \ ; \ \mathrm{Nr}(q) = 1\}.$$

Comme $a > 0$, on a $\mathcal{H}(a,b) \otimes_{\mathbb{Q}} \mathbb{R} = \mathcal{M}_2(\mathbb{R})$, i.e. $\mathcal{H}(a,b)$ met sur $\mathcal{M}_2(\mathbb{R})$ une structure rationnelle non standard. Et on a $\rho(\Gamma) \leq SL_2(\mathbb{R})$.

Proposition

Si $\mathcal{H}(a,b)$ est comme ci-dessus, alors $\Gamma \simeq \rho(\Gamma)$ est un sous-groupe discret de $SL_2(\mathbb{R})$ et $\Gamma \backslash SL_2(\mathbb{R})$ est compact.

Remarque

Si $\mathcal{H}(a,b) \simeq \mathcal{M}_2(\mathbb{Q})$, alors ceci donne les sous-groupes arithmétiques de $SL_2(\mathbb{R})$ commensurables à $SL_2(\mathbb{Z})$.

Groupes modulaires de Hilbert

Soient $d \in \mathbb{N}^* \setminus (\mathbb{Z}^*)^2$ et $\mathbb{F} := \mathbb{Q}(\sqrt{d})$ corps quadratique. On a deux plongements réels et aucun complexe et $SL_2(\mathbb{C})$ est défini sur $\mathbb{F}$. $\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(SL_2)$ est défini sur $\mathbb{Q}$ et de $\mathbb{Q}$-rang 1 et on a

$$(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}} SL_2)(\mathbb{R}) = SL_2(\mathbb{R}) \times SL_2(\mathbb{R}).$$

Le groupe arithmétique $\Gamma := SL_2(\mathcal{O}_{\mathbb{F}})$ est un sous-groupe discret de $SL_2(\mathbb{R})^2$, appelé *groupe modulaire de Hilbert*. L'action $\Gamma \curvearrowright \mathbb{H}^2$ sur le plan hyperbolique est propre et $\Gamma\backslash\mathbb{H}^2$ est de volume fini. C'est la *surface modulaire de Hilbert* associée à $\mathbb{F}$.

Géométrie de $\Gamma\backslash\mathbb{H}^2 \leftrightarrow$ propriétés de $\mathbb{F}$. Exemple : $\#\{\text{bouts de } \Gamma\backslash\mathbb{H}^2\} = \text{nombre de classes de } \mathbb{F}$.

Plus généralement, on peut considérer $[\mathbb{F} : \mathbb{Q}] = d$ avec $\mathbb{F}$ totalement réel. Alors $\Gamma := SL_2(\mathcal{O}_{\mathbb{F}}) \leq SL_2(\mathbb{R})^d$ discret et on a $\Gamma\backslash\mathbb{H}^d$.

Groupes de Bianchi

$d \in \mathbb{N}^* \setminus (\mathbb{Z}^*)^2$ et $\mathbb{F} := \mathbb{Q}(\sqrt{-d})$. $\mathrm{Res}_{\mathbb{F}/\mathbb{Q}}(SL_2)$ est défini sur $\mathbb{Q}$, de $\mathbb{Q}$-rang 1 et

$$(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}} SL_2)(\mathbb{R}) = SL_2(\mathbb{C}).$$

Le sous-groupe discret $\Gamma := SL_2(\mathcal{O}_{\mathbb{F}}) \leq SL_2(\mathbb{C})$ est discret, appelé *groupe de Bianchi*.

L'espace symétrique $X = G/K$ $(G = SL_2(\mathbb{C}))$ est l'espace hyperbolique de dim 3 :

$$\mathbb{H}^3 = \{(x, y, t) \in \mathbb{R}^3 \ ; \ t > 0\} \text{ et } ds^2 = \frac{dx^2 + dy^2 + dt^2}{t^2}.$$

$SL_2(\mathcal{O}_{\mathbb{F}})\backslash\mathbb{H}^3$ exemple typique de variété hyperbolique non-compacte, arithmétique et de volume fini, de dim 3. Il existe aussi des sous-groupes co-compacts arithmétiques de $SL_2(\mathbb{C})$, construits via des algèbres de quaternions sur $\mathbb{F}$...

Groupes modulaires de Picard

- Corps quadratiques réels $\rightsquigarrow$ groupes modulaires de Hilbert.
- Corps quadratiques imaginaires $\rightsquigarrow$ groupes modulaires de Picard.

Ces derniers motivés par les équations différentielles à singularités régulières (en 2 variables) et exemples importants pour le programme de Langlands.

Comme Bianchi, mais avec $SU(2,1)$ à la place de SL_2. Soit la forme hermitienne $\langle \cdot, \cdot \rangle$ sur $\mathbb{C}^3$ définie par

$$\langle z, w \rangle = \overline{z_1} w_1 + \overline{z_2} w_2 - \overline{z_3} w_3.$$

On considère

$$SU(2,1) := \{ g \in SL_3(\mathbb{C}) \ ; \ \langle gz, gw \rangle = \langle z, w \rangle \ , \ \forall z, w \in \mathbb{C}^3 \}.$$

Groupes modulaires de Picard

$SU(2,1)$ défini sur $\mathbb{Q}$, donc sur $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$ ($q \in \mathbb{N}^* \setminus (\mathbb{N}^*)^2$).
$\mathrm{Res}_{\mathbb{F}/\mathbb{Q}} SU(2,1)$ défini sur $\mathbb{Q}$, de $\mathbb{Q}$-rang 1 et

$$(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}} SU(2,1))(\mathbb{R}) = SU(2,1)(\mathbb{C}).$$

Le groupe arithmétique $\Gamma := SU(2,1)(\mathcal{O}_{\mathbb{F}}) \leq SU(2,1)$ est le *groupe modulaire de Picard* associé à $\mathbb{F}$. Si $G := SU(2,1)$, alors

$$X := G/K = SU(2,1)/S(U(1) \times U(1))$$

$$\simeq B^2_{\mathbb{C}} = \{(z,w) \in \mathbb{C}^2 \ ; \ |z|^2 + |w|^2 \leq 1\}$$

et $SU(2,1)(\mathcal{O}_{\mathbb{F}}) \backslash B^2_{\mathbb{C}}$ est la *surface modulaire de Picard* de $\mathbb{F}$.

Groupes modulaires de Picard généralisés

V un ev de dim 3 sur $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$. $L \subset V$ un $\mathcal{O}_{\mathbb{F}}$-réseau et $J : V \times V \to \mathbb{F}$ une forme hermitienne non-dégénérée sur V à valeurs dans $\mathcal{O}_{\mathbb{F}}$ sur L, en particulier, $J(u,v) = \sigma(J(v,u))$ avec $\{1, \sigma\} = \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ et $J(au, bv) = \sigma(a)bJ(u,v)$. On suppose $\mathrm{sign}(J) = (2,1)$.

$$SU(J, V\otimes\mathbb{C}) = \{g \in SL(V\otimes\mathbb{C}) \,;\, J(gu, gv) = J(u,v),\ \forall u, v \in V\otimes\mathbb{C}\}.$$

est défini sur $\mathbb{F}$ et

$$(\mathrm{Res}_{\mathbb{F}/\mathbb{Q}} SU(J, V\otimes\mathbb{C}))(\mathbb{R}) = SU(2,1)(\mathbb{C}).$$

Le groupe $\Gamma := \{g \in (\mathrm{Res}_{\mathbb{F}/\mathbb{Q}} SU(J, V\otimes\mathbb{C}))(\mathbb{Q}) \,;\, gL = L\}$ est le *groupe modulaire de Picard* de (V, J, L).

En particulier, les surfaces de Picard $\Gamma\backslash B^2_{\mathbb{C}}$ sont importantes car espaces loc. symétriques de mêmes $\mathbb{Q}$-rang et $\mathbb{R}$-rang, égal à 1.

Références I

L. Ji.
Lectures on locally symmetric spaces and arithmetic groups.
University of Michigan, 2004.

A. Borel.
Introduction aux groupes arithmétiques.
Hermann, 1969.

A. Borel.
Linear algebraic groups.
Springer-Verlag, 1969.

E. Freitag.
Hilbert modular forms.
Springer-Verlag, 1990.

Références II

I. Gelfand, M. Graev, and I. Pisteskii-Shapiro.
Representation theory and automorphic functions.
Sunders Company, 1968.

R. Holzapfel.
Geometry and arithmetic around Euler partial differential equations.
Reidel Publishing Company, 1968.

S. Katok.
Fuchsian groups.
University of Chicago Press, 1992.

Références III

R. Langlands and D. Ramakrishnan.
The zeta functions of Picard modular surfaces.
Les publications CRM, Montreal, 1992.

C. Maclachlan and A. Reid.
The arithmetic of hyperbolic 3-manifolds.
Springer-Verlag, 2003.

V. Platonov and A. Rapinchuk.
Algebraic groups and number theory.
Academic Press, 1994.

G. van der Geer.
Hilbert modular surfaces.
Springer-Verlag, 1988.

Merci !