[1959a] Adèles et groupes algébriques

On désignera toujours par k, soit un corps de nombres algébriques, soit un corps de fonctions algébriques de dimension 1 sur un corps de constantes fini. On désignera par k_v le complété de k par rapport à une valuation v; si une valuation est discrète, on la désignera le plus souvent par un symbole tel que $\mathfrak{p}$, et on désignera par $r_\mathfrak{p}$ l'anneau des entiers $\mathfrak{p}$-adiques dans $k_\mathfrak{p}$. On désignera par S tout ensemble fini de valuations de k, contenant l'ensemble S_0 des valuations non discrètes (pour lesquelles le complété est $\mathbf{R}$ ou $\mathbf{C}$); bien entendu S_0 est vide si k est un corps de fonctions.

Si V est une variété algébrique, définie sur un corps k, on identifiera, suivant l'usage, V avec l'ensemble des points de V sur le domaine universel, et on notera V_k l'ensemble des points de V rationnels sur k. Cette convention s'appliquera notamment si V est une variété de groupe, une variété d'algèbre, une variété de corps, etc.; on dira par exemple que V est une variété d'algèbre de dimension n, définie sur k, si, en tant que variété, c'est un espace affine de dimension n, sur lequel on s'est donné, outre la structure additive usuelle, une structure multiplicative, c'est-à-dire une application bilinéaire (toujours supposée associative) de $V \times V$ dans V, définie sur k; V_k est alors une algèbre sur k au sens usuel; si V_k est un corps (donc, au sens usuel, une extension de k de degré n), on dit que V est une variété de corps de dimension n sur k. Cette manière de parler est conforme à l'usage ancien de Kronecker, Hilbert, etc. (qui ne se gênaient pas pour parler de l'élément générique d'un corps).

1. Soit V une variété définie sur k; V_{k_v} peut être munie, d'une manière évidente, d'une topologie qui la rend localement compacte, et compacte si V est complète (on commence par le cas où V est une variété affine, V_{k_v} étant alors considérée comme partie fermée d'un espace vectoriel de dimension finie sur k_v; on passe de là d'une manière évidente au cas d'une variété abstraite quelconque).

Soit $\mathfrak{p}$ une valuation discrète de k. Si V est une variété affine, on notera $V_{r_\mathfrak{p}}$ l'ensemble des points de $V_{k_\mathfrak{p}}$ dont les coordonnées sont dans $r_\mathfrak{p}$; il est immédiat que c'est une partie compacte de $V_{k_\mathfrak{p}}$. Plus généralement, soit V une variété abstraite, définie sur k; on sait que V admet toujours un recouvrement *fini* par des ouverts isomorphes à des variétés affines $V^{(i)}$, définies aussi sur k; autrement dit, on peut écrire $V = \bigcup_i f_i(V^{(i)})$, où les f_i sont des isomorphismes (définis sur k) des variétés affines $V^{(i)}$ sur des ouverts de V (au sens de la topologie de Zariski, bien entendu). Pour toute valuation discrète $\mathfrak{p}$ de k, posons:

$$V_{r_\mathfrak{p}} = \bigcup_i f_i(V^{(i)}_{r_\mathfrak{p}});$$

c'est là une partie compacte de $V_{k_\mathfrak{p}}$. Posons maintenant, pour tout ensemble fini S

de valuations de k contenant l'ensemble S_0 des valuations non discrètes:

$$V_S = \prod_{v \in S} V_{k_v} \times \prod_{\mathfrak{p} \notin S} V_{r_\mathfrak{p}},$$

où le second produit est étendu à toutes les valuations de k (nécessairement discrètes) qui n'appartiennent pas à S; c'est là une partie localement compacte de $\prod_v V_{k_v}$, et on a $V_S \subset V_{S'}$ pour $S \subset S'$. *On désignera par $V_{\mathbf{A}_k}$ la limite inductive des* V_S, c'est-à-dire la réunion des V_S munie de la topologie pour laquelle un système fondamental d'ouverts est formé par la réunion de l'ensemble des ouverts dans tous les V_S. *Cette notion est justifiée par le fait que $V_{\mathbf{A}_k}$ est définie d'une manière intrinsèque*, c'est-à-dire ne dépend pas de la manière dont on a écrit V comme réunion finie d'images isomorphes de variétés affines; la vérification de cette assertion est élémentaire. On appelera $V_{\mathbf{A}_k}$ *l'espace adélique* associé à V. Au lieu de $\mathbf{A}_k$, on écrira souvent $\mathbf{A}$ quand aucune confusion n'est possible. L'espace adélique associé à la droite affine n'est autre que l'ensemble des adèles (dits aussi "répartitions" ou "valuation-vectors") du corps k, avec sa topologie usuelle: cet ensemble (muni de sa structure topologique, et de sa structure d'anneau) sera noté $\mathbf{A}_k$, ou simplement $\mathbf{A}$.

La notion d'espace adélique possède des propriétés fonctorielles raisonnables. Si f est une application partout définie d'une variété V dans une variété W, définie sur k, on en déduit d'une manière évidente une application continue de $V_\mathbf{A}$ dans $W_\mathbf{A}$. Si par exemple on s'est donné sur V une loi de groupe algébrique, on en déduit une loi de groupe sur $V_\mathbf{A}$, et $V_\mathbf{A}$ s'appellera le groupe adélique associé à V. Par exemple, si V est le groupe *multiplicatif G_m à une variable* sur k, le groupe adélique correspondant est le *groupe des idèles* de k au sens usuel. Si l'application f de V dans W est surjective, il n'en est pas de même, en général, de l'application de $V_\mathbf{A}$ dans $W_\mathbf{A}$ qui lui est associée. Cependant, si V est un fibré de base W, localement trivial sur k, au sens de la géométrie algébrique, et si f est la projection de V sur sa base W, alors l'application correspondante de $V_\mathbf{A}$ dans $W_\mathbf{A}$ est surjective. En particulier, si G est un groupe et g un sous-groupe de G, tous deux définis sur k, et qu'on pose $H = G/g$, l'application de $G_\mathbf{A}$ dans $H_\mathbf{A}$, associée à l'application canonique de G sur H, n'est pas surjective en général; mais, *si G est* (sur le corps de base k) *fibré localement trivial sur $H = G/g$, alors on peut identifier canoniquement $H_\mathbf{A}$ avec $G_\mathbf{A}/g_\mathbf{A}$.*

2. Soit K une extension séparable de k, de degré fini d; soit V une variété affine ou projective de dimension n, définie sur K; on va indiquer comment on peut associer à ces données une variété W de dimension nd, définie sur k, et qui, sur le domaine universel, est isomorphe au produit de V et de ses conjuguées sur k. Pour fixer les idées, considérons le cas affine. Alors V est définie par des équations:

$$P_\mu(X_1, \ldots, X_N) = 0 \qquad (1 \leq \mu \leq m),$$

à coefficients dans K. Soit $(a_1, \ldots, a_d)$ une base de K sur k; posons:

$$X_i = \sum_{j=1}^{d} a_j Y_{ji} \qquad (1 \leq i \leq N)$$

les Y_{ji} étant de nouvelles indéterminées; alors les P_μ deviennent des polynômes à coefficients dans K par rapport aux Y_{ji}, et peuvent donc s'écrire:

$$P_\mu(X_1, \ldots, X_N) = \sum_{h=1}^{d} a_h Q_{h\mu}(Y_{11}, \ldots, Y_{dN}),$$

où les $Q_{h\mu}$ sont des polynômes à coefficients dans k. Dans ces conditions, W est la variété définie par les équations

$$Q_{h\mu}(Y_{11}, \ldots, Y_{dN}) = 0 \qquad (1 \leq h \leq d, 1 \leq \mu \leq m)$$

dans l'espace affine de dimension dN. En effet, une vérification facile montre qu'après un changement de coordonnées *linéaire*, à coefficients dans le corps composé de K et de tous ses conjugués sur k, ces équations sont précisément celles qui définissent le produit de V et de ses conjuguées sur k. C'est d'ailleurs seulement cette dernière vérification qui exige que K soit séparable sur k; s'il ne l'était pas, les définitions ci-dessus auraient encore un sens, mais définiraient une opération ayant des propriétés assez différentes de celles qui nous intéressent ici.

On dira, dans les circonstances ci-dessus, que W est déduite de V par *restriction* du corps de base de K à k, et on écrira $W = \mathfrak{R}_{K\to k}(V)$. Il est immédiat qu'il y a correspondance biunivoque (canonique!) entre V_K et W_k. On vérifie aussi, sans difficulté, qu'il y a correspondance biunivoque (non moins canonique) entre $V_{\mathbf{A}_K}$ et $W_{\mathbf{A}_k}$. Cela permet, par exemple, dans tous les problèmes relatifs aux espaces adéliques sur les corps de nombres, de se ramener, si l'on veut, au cas où le corps de base est $\mathbf{Q}$.

3. Soit G une variété de groupe de dimension n, définie sur k. Il existe sur G une forme différentielle ω de degré n, invariante à gauche, définie sur k, et ω est unique à un facteur près (facteur qui doit être dans k); si $x_1, \ldots, x_n$ sont des fonctions sur G, définies sur k, qui soient des coordonnées locales dans un voisinage de l'élément neutre e (et, pour fixer les idées, nulles en e), on pourra écrire

$$\omega = y\, dx_1 \ldots dx_n,$$

où y est une fonction sur G, définie sur k, et finie en e. On va montrer comment, si v est une valuation quelconque de k, on peut associer à ω une mesure de Haar bien déterminée sur G_{k_v}, mesure qu'on notera $|\omega|_v$. Pour cela on distinguera trois cas:

(a) $k_v = \mathbf{R}$; alors les x_i peuvent servir de coordonnées locales sur G_{k_v} au voisinage de e; au voisinage de e, est fonction analytique réelle de $x_1, \ldots, x_n$; dans ces conditions, $y\, dx_1 \ldots dx_n$ peut s'interpréter comme une forme différentielle au sens usuel sur G_{k_v} au voisinage de e; comme il est clair qu'elle est invariante à gauche, elle définit par translation une mesure de Haar sur G_{k_v}, qu'on note $|\omega|_v$.

(b) $k_v = \mathbf{C}$: les x_i sont alors des coordonnées locales complexes sur G_{k_v} au voisinage de e, et y est fonction analytique complexe des x_i au voisinage de e; on prendra $|\omega|_v = i^n y\bar{y}\, dx_1\, \overline{dx_1} \ldots dx_n\, \overline{dx_n}$.

(c) Soit $\mathfrak{p}$ une valuation discrète; $G_{k_\mathfrak{p}}$ est une variété analytique sur le corps valué complet $k_\mathfrak{p}$; comme précédemment, $x_1, \ldots, x_n$ peuvent être considérées comme coordonnées locales au voisinage de e sur $G_{k_\mathfrak{p}}$, c'est-à-dire qu'elles déterminent un homéomorphisme d'un voisinage de e dans $G_{k_\mathfrak{p}}$ sur un voisinage de 0 dans l'espace $k_{\mathfrak{p}}^n$. Convenons, sur le groupe additif $k_{\mathfrak{p}}$, de noter $|dx|_{\mathfrak{p}}$ la mesure de Haar, normée par la condition que $r_{\mathfrak{p}}$ (anneau des entiers $\mathfrak{p}$-adiques) soit de mesure 1; la mesure de Haar dans $k_{\mathfrak{p}}^n$, produit des mesures $|dx|_{\mathfrak{p}}$ sur les n facteurs, sera notée $|dx_1 \cdots dx_n|_{\mathfrak{p}}$. On posera alors, au voisinage de e:

$$|\omega|_{\mathfrak{p}} = |y|_{\mathfrak{p}} |dx_1 \ldots dx_n|_{\mathfrak{p}},$$

où $|y|_{\mathfrak{p}}$ est la valeur absolue $\mathfrak{p}$-adique de la valeur de y au point considéré (y est, comme précédemment, fonction analytique de $x_1, \ldots, x_n$ au voisinage de e, ce qui veut dire qu'on peut l'écrire comme série convergente de puissances de $x_1, \ldots, x_n$). Naturellement, la valeur absolue $\mathfrak{p}$-adique est normée de la manière usuelle, c'est-à-dire de façon que l'automorphisme $x \to ax$ du groupe additif de $k_{\mathfrak{p}}$ multiplie la mesure de Haar par le facteur $|a|_{\mathfrak{p}}$.

Les définitions ci-dessus se justifient du fait qu'elles sont indépendantes du choix des coordonnées locales $x_1, \ldots, x_n$ au voisinage de e; c'est évident dans les cas (a) et (b), en vertu de la formule de changement de variables dans les intégrales multiples en analyse classique, et cela résulte immédiatement, dans le cas (c), de la formule correspondante en analyse $\mathfrak{p}$-adique (qui se démontre encore plus facilement qu'en analyse classique).

De ce qui précède, on peut, dans certain cas, déduire la définition d'une mesure de Haar sur le groups adélique $G_{\mathbf{A}}$ attaché à G. En se reportant au paragraphe 1, il est évident que cela est possible chaque fois que, sur le produit

$$G_S = \prod_{v \in S} G_{k_v} \times \prod_{\mathfrak{p} \notin S} G_{r_{\mathfrak{p}}},$$

il existe une mesure produit des mesures $|\omega|_v$; car il est évident que les mesures ainsi définies sur G_S et sur $G_{S'}$, pour $S \subset S'$, coïncident sur G_S. Or, pour que la mesure en question soit définie, il faut et il suffit que le produit infini

$$\prod_{\mathfrak{p}} \int_{G_{r_{\mathfrak{p}}}} |\omega|_{\mathfrak{p}},$$

étendu à toutes les valuations discrètes de k, soit absolument convergent. Lorsqu'il en est ainsi, on notera $\prod_v |\omega|_v$ la mesure ainsi obtenue. *On observera que celle-ci ne dépend pas du choix de* ω; en effet, si on remplace ω par $c\omega$, avec $c \in k^\times$, elle se multiplie par $\prod_v |c|_v$, qui est 1 ("formule du produit" d'Artin; rappelons que celle-ci se démontre comme suit: $x \to cx$ est un automorphisme du groupe additif $\mathbf{A}_k$, qui multiplie la mesure de Haar par $\prod_v |c|_v$, et qui d'autre part induit un automorphisme sur k considéré comme sous-groupe de $\mathbf{A}_k$, donc, par passage au quotient, détermine un automorphisme du groupe *compact* $\mathbf{A}_k/k$ et par suite laisse invariante toute mesure de Haar sur ce dernier; k étant discret dans $\mathbf{A}_k$, $\mathbf{A}_k$ et $\mathbf{A}_k/k$ sont localement isomorphes, donc les mesures de Haar y prennent le même facteur).

On dira que G a la *propriété de convergence* si $\prod_v |\omega|_v$ y est défini; le cas où le produit infini écrit ci-dessus, sans être absolument convergent, est convergent lorsque les $\mathfrak{p}$ sont ordonnés "naturellement" (c'est-à-dire par ordre de grandeur croissante des normes) est intéressant aussi; lorsqu'il en est ainsi, on dira que G a la *propriété de convergence relative*. Les exemples assez variés qu'on a traités jusqu'ici rendent assez plausibles les conjectures suivantes: pour que G ait la propriété de convergence relative, il faut et il suffit que G n'admette pas d'homomorphisme sur G_m, défini sur k; pour que G ait la propriété de convergence, il faut et il suffit que G n'admette pas d'homomorphisme sur G_m, défini sur le domaine universel. En particulier, tous les groupes unipotents, et tous les groupes semi-simples qu'on a pu traiter de ce point de vue, ont la propriété de convergence. Le groupe G_m n'a pas la propriété de convergence relative.

Le groupe adélique attaché au groupe additif G_a à une variable n'est autre que le groupe additif de $\mathbf{A}_k$; ce groupe a évidemment la propriété de convergence. Nous poserons:

$$\mu_k = \int_{\mathbf{A}_k/k} \prod_v |dx|_v$$

(on convient, une fois pour toutes, d'identifier d'une manière évidente une mesure de Haar sur un groupe localement compact Γ avec celle qu'elle détermine par passage au quotient sur l'espace homogène Γ/γ, lorsque γ est un sous-groupe discret quelconque de Γ). On voit facilement que $\mu_k = |\Delta|^{1/2}$, où Δ est le discriminant de k, lorsque k est un corps de nombres algébriques, et que $\mu_k = q^{g-1}$ si k est un corps de fonctions de genre g sur un corps de constantes à q éléments.

Soit alors G un groupe de dimension n sur k, ayant la propriété de convergence; nous poserons:

$$\Omega_G = \mu_k^{-n} \prod_v |\omega|_v,$$

et nous dirons que c'est la *mesure de Tamagawa* sur $G_{\mathbf{A}}$. Il résulte de ce qui précède que cette mesure est déterminée d'une manière unique (elle ne dépend pas du choix de ω).

Soit K une extension séparable de k, de degré fini. Soit G un groupe défini sur K; soit G' le groupe $\mathfrak{R}_{K\to k}(G)$, déduit de G par restriction du corps de base de K à k; on a déjà observé que $G_{\mathbf{A}_K}$ s'identifie canoniquement à $G'_{\mathbf{A}_k}$; on vérifie facilement que G et G' ont simultanément la propriété de convergence, et que les mesures de Tamagawa Ω_G (sur $G_{\mathbf{A}_K}$) et $\Omega_{G'}$ (sur $G'_{\mathbf{A}_k}$) coïncident lorsqu'on identifie ces groupes. C'est, entre autres, pour qu'il en soit ainsi qu'on a introduit le facteur μ_k^{-n} dans la définition de Ω_G.

4. Toujours avec les mêmes notations, G_k s'identifie d'une manière évidente avec un sous-groupe discret de $G_{\mathbf{A}}$; on dit que c'est le groupe des adèles *principaux* de G. On s'est aperçu, dans ces derniers temps, qu'une bonne partie des résultats les plus importants de l'arithmétique classique pouvait s'exprimer en énonçant des propriétés de $G_{\mathbf{A}}/G_k$ pour des groupes algébriques G convenables; cette observation, faite d'abord par Chevalley, comme chacun sait, pour le cas particulier du groupe des idèles (groupe G_m), est d'une importance capitale; le mérite semble en revenir principalement à Ono et Tamagawa. Le cas où G est commutatif est celui de la théorie classique des corps de nombres algébriques; celui où G est le groupe orthogonal est celui de la théorie des formes quadratiques; il semble donc qu'on touche au moment où ces deux théories, confondues à leurs débuts (la théorie des formes quadratiques binaires ne différant pas de celle des corps quadratiques), vont enfin se fondre de nouveau en une seule, à savoir la théorie arithmétique des groupes algébriques.

Il n'est pas difficile de démontrer (cf. Ono [1]) que $G_{\mathbf{A}}/G_k$ est compact lorsque G est unipotent. Il en est de même, d'autre part, pour certains groupes semi-simples; en voici deux cas typiques:

a. G est le groupe des éléments de norme 1 sur le centre dans une variété de corps non commutatif;

b. G est le groupe orthogonal d'une forme quadratique ne représentant pas 0. Même lorsque $G_{\mathbf{A}}/G_k$ n'est pas compact, il peut arriver que cet espace soit de mesure finie (pour une mesure de Haar quelconque sur $G_{\mathbf{A}}$); il semble plausible qu'il en soit ainsi pour les mêmes groupes dont on a conjecturé plus haut qu'ils ont la propriété de convergence relative. En tout cas, au moyen de la réduction des formes quadratiques, on a pu démontrer cette propriété pour un grand nombre de groupes semi-simples, et Ramanathan a annoncé qu'il possédait une démonstration s'appliquant à tous les groupes semi-simples "classiques".

Plaçons-nous dans le cas où G a la propriété de convergence; nous poserons:

$$\tau(G) = \int_{G_{\mathbf{A}}/G_k} \Omega_G,$$

et nous appellerons $\tau(G)$, lorsqu'il est fini, le *nombre de Tamagawa* de G. Le mérite essentiel de Tamagawa consiste à avoir défini $\tau(G)$, d'abord dans le cas particulier où G est le groupe orthogonal d'une forme quadratique (sur le corps des rationnels, puis sur un corps de nombres algébriques), et à avoir reconnu les faits suivants:

a. Pour ce groupe (plus précisément, pour la composante connexe de l'élément neutre dans ce groupe), on a $\tau(G) = 2$;

b. La formule $\tau(G) = 2$ est entièrement équivalente à l'ensemble des résultats des trois célèbres mémoires de Siegel sur les formes quadratiques (C. L. Siegel, Über die analytische Theorie der quadratischen Formen [2], soit 194 pages, qui ne contiennent même pas une démonstration complète pour le cas général des formes de signature quelconque sur un corps quelconque).

En fait, une fois qu'on a eu l'idée d'exprimer les choses dans ce langage, l'équivalence de la formule $\tau(G) = 2$ avec les résultats de Siegel n'est pas trop difficile à vérifier. Naturellement, Tamagawa ne s'est pas arrêté là. Il a d'abord cherché à rédiger, dans ce même langage, la démonstration même du théorème de Siegel (l'idée de traduire celle-ci dans le langage des idèles était déjà venue à M. Kneser il y a quelques années, mais celui-ci n'avait rien publié sur ce sujet). Un avantage essentiel de la nouvelle méthode consiste en ce que le théorème à démontrer est, du fait même de son énoncé, birationnellement invariant, alors que chez Siegel (et, avant lui, chez Minkowski) il apparaissait comme lié à un "genre" de formes quadratiques. En particulier, en vertu des isomorphismes bien connus entre groupes classiques, les cas $n = 3$ et $n = 4$ se ramènent ainsi à des questions analogues sur les algèbres de quaternions, qu'on sait traiter directement; or c'était justement les cas qui donnaient le plus de difficulté chez Siegel. Ces cas étant acquis, tout le reste de la démonstration peut maintenant se présenter fort simplement, et presque sans calculs.

D'autre part, on a commencé à examiner d'autres groupes semi-simples: groupe spin (Tamagawa), groupes linéaire spécial et projectif sur une algèbre simple, etc. Dans tous les cas qu'on a su traiter, on a trouvé que $\tau(G)$ *est un entier, et qu'il est égal à* 1 *lorsque* G *est un groupe semi-simple "simplement connexe"* (au sens algébrique, c'est-à-dire que tout groupe isogène à G est une image homomorphe de G). Il en est bien ainsi, par exemple, si G est le groupe des éléments de norme 1 sur le centre dans une variété d'algèbre simple sur un corps de nombres ou bien sur un corps de fonctions.

Bibliographie

1. Ono, Takashi. Sur une propriété arithmétique des groupes algébriques commutatifs, Bull. Soc. math. France, t. 85, 1957, p. 307–323.
2. Siegel, Carl Ludwig. Über die analytische Theorie der quadratischen Formen, I: Annals of Math., t. 36, 1935, p. 527–606; II: t. 37, 1936, p. 230–263; III: t. 38, 1937, p. 212–291.
3. Tamagawa, Tsuneo, Mémoire à paraître aux Annals of Mathematics.